

## CUBE SUM PROBLEM AND AN EXPLICIT GROSS-ZAGIER FORMULA

LI CAI, JIE SHU, AND YE TIAN

## CONTENTS

1. Introduction and Main Results	1
2. Nontriviality of Heegner Points	6
3. An Explicit Gross-Zagier Formula	12
References	19

## 1. INTRODUCTION AND MAIN RESULTS

We call a nonzero rational number a *cube sum* if it is of form  $a^3 + b^3$  with  $a, b \in \mathbb{Q}^\times$ . Similar to Heegner's work on congruent number problem, Satgé [23] showed that if  $p \equiv 2 \pmod{9}$  (resp.  $p \equiv 5 \pmod{9}$ ) is a prime, then  $2p$  (resp.  $2p^2$ ) is a cube sum. Lieman [16] showed there are infinitely many cube-free integers which are not cube sums. Sylvester [24] showed there are infinitely many integers with at most 2 distinct prime factors which are not cube sums. The following is one of main results in this paper.

**Theorem 1.1.** *For any odd integer  $k \geq 1$ , there exist infinitely many cube-free odd integers  $n$  with exactly  $k$  distinct prime factors such that  $2n$  is a cube sum (resp. not a cube sum).*

For any  $n \in \mathbb{Q}^\times$ , let  $C^{(n)}$  be the elliptic curve over  $\mathbb{Q}$  defined by the equation  $x^3 + y^3 = 2n$ . Note that the torsion part of the Mordell-Weil group  $C^{(n)}(\mathbb{Q})$  is trivial unless  $2n$  is a cube, which is not a cube sum by our convention. Then  $2n$  is a cube sum if and only if the rank of the Mordell-Weil group  $C^{(n)}(\mathbb{Q})$  is positive.

For an odd prime  $p \equiv 2, 5 \pmod{9}$ , denote  $p^* = p^{\pm 1} \equiv 2 \pmod{9}$ . To prove that  $p^*$  is a cube sum, Satgé [23] constructed a non-trivial Heegner point on  $C^{(p^*)}$  (see also Dasgupta and Voight [6].) In this paper, we give a similar construction of Heegner point on  $C^{(p^*)}$  and relate its height to some special  $L$ -value. Together with work of Kolyvagin [14], Perrin-Riou [20] and Kobayashi [13], we have the following result on the Birch and Swinnerton-Dyer conjecture for  $C^{(p^*)}$  and  $C^{(p^{*-1})}$ .

**Theorem 1.2.** *Let  $p \equiv 2, 5 \pmod{9}$  be an odd prime number. Then  $2p^*$  is a cube sum. Moreover,*

- (1)  $\text{ord}_{s=1} L(s, C^{(p^*)}) = \text{rank}_{\mathbb{Z}} C^{(p^*)}(\mathbb{Q}) = 1$  and  $\text{ord}_{s=1} L(s, C^{(p^{*-1})}) = \text{rank}_{\mathbb{Z}} C^{(p^{*-1})}(\mathbb{Q}) = 0$ .
- (2) *The Tate-Shafarevich groups  $\text{III}(C^{(p)})$  and  $\text{III}(C^{(p^{-1})})$  are finite, and, for any prime  $\ell \nmid 2p$ , the  $\ell$ -part of  $\#\text{III}(C^{(p)}) \cdot \#\text{III}(C^{(p^{-1})})$  is as predicted by the Birch and Swinnerton-Dyer conjecture for  $C^{(p)}$  and  $C^{(p^{-1})}$ .*

In this paper, we give also a general construction of Heegner point and obtain an explicit Gross-Zagier formula, which is a variant of our previous work [3] and is used to prove Theorem 1.2.

Let  $\phi$  be a newform of weight 2, level  $\Gamma_0(N)$ , with Fourier expansion  $\phi = \sum_{n=1}^{\infty} a_n q^n$  normalized such that  $a_1 = 1$ . Let  $K$  be an imaginary quadratic field of discriminant  $D$  with  $\mathcal{O}_K$  its ring of integers. For an positive integer  $c$ , let  $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$  be the order of  $K$  of conductor  $c$ . Denote by  $H_c$  the ring class field of  $K$  which is the abelian extension over  $K$  characterized by the property that the Artin map induces an isomorphism  $\text{Pic}(\mathcal{O}_c) \xrightarrow{\sim} \text{Gal}(H_c/K)$ . Here  $\text{Pic}(\mathcal{O}_c)$  is the Picard group for invertible (fractional)  $\mathcal{O}_c$ -ideals. Let  $\chi : \text{Gal}(H_c/K) \rightarrow \mathbb{C}^\times$  be a primitive character of ring class field. Let  $L(s, \phi, \chi)$  be the Rankin-Selberg  $L$ -function of  $\phi$  and  $\chi$  which is defined by an Euler product over primes  $p$

$$L(s, \phi, \chi) = \prod_{p < \infty} L_p(s, \phi, \chi).$$

Li Cai was supported by the Special Financial Grant from the China Postdoctoral Science Foundation 2014T70067; Ye Tian was supported by the 973 Program 2013CB834202 and NSFC grants 11325106, 11321101, and 11031004.

We refer to [9] for the general definition of the local factors  $L_p(s, \phi, \chi)$ . Denote by  $S$  the set of finite primes  $p|(N, Dc)$  such that if  $p|N$  then  $p|c$ . For any  $p \notin S$ , the local factor  $L_p(s, \phi, \chi) = \prod_{1 \leq i, j \leq 2} (1 - \alpha_{p,i} \beta_{p,j} p^{-s})^{-1}$  where  $\alpha_{p,i}$  and  $\beta_{p,j}$  are local parameters of  $L$ -series  $L(s, \phi)$  and  $L(s, \chi)$ :

$$\prod_{i=1,2} (1 - \alpha_{p,i} p^{-s}) = L_p(s, \phi)^{-1} = \begin{cases} 1 - a_p p^{-s} + p^{1-2s}, & \text{if } p \nmid N; \\ 1 - a_p p^{-s}, & \text{if } p|N; \\ 1, & \text{if } p^2|N, \end{cases}$$

and

$$\prod_{j=1,2} (1 - \beta_{p,j} p^{-s}) = L_p(s, \chi)^{-1} = \begin{cases} \prod_{\mathfrak{p}|p} (1 - \chi([\mathfrak{p}]) N \mathfrak{p}^{-s}), & \text{if } p \nmid c; \\ 1, & \text{if } p|c, \end{cases}$$

where  $[\mathfrak{p}] \in \text{Pic}(\mathcal{O}_c)$  is the ideal class of the prime  $\mathfrak{p}|p$ . The  $L$ -function  $L(s, \phi, \chi)$  admits an analytically continuation to the whole  $s$ -plane with the functional equation

$$G_2(s)^2 L(s, \phi, \chi) = \epsilon(s, \phi, \chi) G_2(2-s)^2 L(2-s, \phi, \chi)$$

where  $G_2(s) := 2(2\pi)^{-s} \Gamma(s)$  and the root number  $\epsilon(\phi, \chi) := \epsilon(1, \phi, \chi) = \pm 1$ .

Firstly, assume that:

- (1)  $(c, N) = 1$ , and if  $p|(N, D)$  then  $\text{ord}_p(N) = 1$  (in particular,  $a_p = \pm 1$ ).
- (2) The set  $\Sigma$  has even cardinality, where  $\Sigma$  consists of prime factors  $p$  of  $N$  satisfying
  - either  $p$  is inert in  $K$  and  $\text{ord}_p(N)$  is odd,
  - or  $p$  is ramified in  $K$  and  $\chi([\mathfrak{p}]) = a_p$  where  $[\mathfrak{p}] \in \text{Pic}(\mathcal{O}_c)$  is the ideal class of the prime ideal  $\mathfrak{p}$  above  $p$ .

The above assumption implies (see Lemma 3.1 in [3]) that the root number  $\epsilon(\phi, \chi)$  of  $L(s, \phi, \chi)$  is  $-1$ . Let  $B$  be the indefinite quaternion algebra defined over  $\mathbb{Q}$  ramified exactly at the set  $\Sigma$ . There is then an  $\mathbb{Q}$ -embedding from  $K$  to  $B$  and we shall fix one from now on. Let  $R$  be an order in  $B$  with discriminant  $N$  such that  $R \cap K = \mathcal{O}_c$ . Such  $R$  exists. Let  $N_B$  be the reduced norm of  $B$ . Put

$$\Gamma = \{\gamma \in R^\times | N_B(\gamma) = 1\}.$$

The group  $\Gamma$  is viewed as a subgroup of  $\text{SL}_2(\mathbb{R})$  via the embedding  $B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$  which is a Fuchsian group of the first kind (See also [17], Theorem 5.2.13). Let  $X_\Gamma$  be the Shimura curve over  $\mathbb{Q}$  associated to  $B$  with level  $\Gamma$ . The curve  $X_\Gamma$  is a geometrically connected projective curve which has the complex uniformization

$$X_\Gamma(\mathbb{C}) = \Gamma \backslash \mathcal{H} \cup \{\text{cusps}\}$$

where  $\mathcal{H}$  is the upper half plane with the linear fractional action of  $\Gamma$ . The set of cusps is non-empty if and only if  $\Sigma = \emptyset$ . Let  $h_0$  be the unique point in  $\mathcal{H}$  fixed by  $K^\times$  and denote by  $P$  the point on  $X_\Gamma(\mathbb{C})$  represented by  $h_0$ . Then by Shimura's reciprocity law, as  $R \cap K = \mathcal{O}_c$ ,  $P$  is defined over the ring class field  $H_c$  over  $K$  of conductor  $c$ .

Let  $L \in \text{Pic}(X_\Gamma)_{\mathbb{Q}}$  be the Hodge class. It is the line bundle whose global sections are holomorphic modular forms of weight two, i.e.

$$L = \omega_{X_\Gamma/\mathbb{Q}} + \sum_{x \in X_\Gamma(\bar{\mathbb{Q}})} (1 - e_x^{-1})x.$$

Here  $\omega_{X_\Gamma/\mathbb{Q}}$  is the canonical bundle of  $X_\Gamma$ ,  $e_x$  is the ramification index of  $x$  in the complex uniformization of  $X_\Gamma$ , i.e. for a cusp  $x$ ,  $e_x = \infty$  and for a non-cusp  $x$ ,  $e_x$  is half of the order of stabilizers of  $x$  in  $\Gamma$ . Let  $\xi = L/\deg L \in \text{Pic}(X_\Gamma)_{\mathbb{Q}}$  be the normalized Hodge class on  $X_\Gamma$  (of degree one). Here  $\deg L$  denotes the degree of  $L$ , which is the volume of  $X_\Gamma(\mathbb{C})$  with respect to the measure  $dx dy/2\pi y^2$ . Let  $J_\Gamma$  be the Jacobian of  $X_\Gamma$ . The degree one class  $\xi$  defines a morphism

$$[\ ] : X_\Gamma(\bar{\mathbb{Q}}) \longrightarrow J_\Gamma(\bar{\mathbb{Q}})_{\mathbb{Q}}, \quad x \longmapsto [x - \xi].$$

Consider the point

$$P_\chi := \sum_{\sigma \in \text{Gal}(H_c/K)} [P - \xi]^\sigma \otimes \chi(\sigma) \in J_\Gamma(H_c)_{\mathbb{C}} := J_\Gamma(H_c)_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}.$$

Let  $\mathbb{T} \subset \text{End}_{\mathbb{Q}}(J_\Gamma)$  be the sub-algebra generated over  $\mathbb{Z}$  by Hecke correspondences  $T_\ell$ , for  $\ell$  prime to  $N$ . Let  $P_\chi^\phi$  be the projection of  $P_\chi \in J_\Gamma(H_c)_{\mathbb{C}}$  to the eigenspace with the eigen character  $\mathbb{T} \rightarrow \mathbb{C}$  defined by  $T_\ell \mapsto a_\ell$ .

**Theorem 1.3.** *Under assumptions (1) and (2) above, we have the following identity*

$$L'(1, \phi, \chi) = 2^{-\mu(N, D)} \cdot \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \hat{h}_K(P_\chi^\phi),$$

where  $\mu(N, D)$  is the number of common prime factors of  $N$  and  $D$ ,  $u = [\mathcal{O}_c^\times : \mathbb{Z}^\times]$  and

$$(\phi, \phi)_{\Gamma_0(N)} = \iint_{\Gamma_0(N) \backslash \mathcal{H}} |\phi(x + iy)|^2 dx dy,$$

and  $\hat{h}_K$  is the Néron-Tate height on  $J_\Gamma(H_c)_\mathbb{C}$  over  $K$ .

Let  $A$  be an abelian variety over  $\mathbb{Q}$  associated to  $\phi$  in the sense that for all primes  $p$ ,

$$L_p(s, A) = \prod_{\sigma: \mathbb{Q}_\phi \hookrightarrow \mathbb{C}} L(s, \phi^\sigma),$$

where  $\mathbb{Q}_\phi \subset \mathbb{C}$  is the subfield generated over  $\mathbb{Q}$  by all Fourier coefficients of  $\phi$ . Then  $M := \text{End}^0(A)$  is a number field over  $\mathbb{Q}$  of degree  $\dim A$ . There exists a unique embedding  $\iota : M \hookrightarrow \mathbb{C}$  satisfying the following property: for any  $p \nmid N$ , if we take  $\ell \neq p$  a prime inert in  $M$ , then under  $\iota$ , the trace of the  $M_\ell$ -linear map defined by the action of the Frobenius element at  $p$  on the  $\ell$ -adic Tate module  $V_\ell(A) := \lim_n A(\bar{\mathbb{Q}})[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$  equals  $a_p$ .

**Definition 1.4.** *A non-constant morphism  $f : X_\Gamma \rightarrow A$  over  $\mathbb{Q}$  is called an admissible modular parametrization if there is an integral multiple of  $\xi$  represented by a divisor  $\sum n_i x_i$  with integral coefficients  $n_i$  such that  $\sum n_i f(x_i)$  is equal to the identity element in  $A(\mathbb{Q})$ .*

**Proposition 1.5** ([3] Proposition 3.8). *There exists an admissible modular parametrization  $f : X_\Gamma \rightarrow A$ . Moreover, if  $f'$  is another admissible modular parametrization, then there exist nonzero integers  $n, n'$  such that  $nf = n'f'$ .*

By the above proposition, we may take an admissible modular parametrization  $f_1 : X_\Gamma \rightarrow A$ . Let  $A^\vee$  be the dual abelian variety of  $A$ . Since  $A^\vee$  is isogeny to  $A$ , there is also an admissible modular parametrization  $f_2 : X_\Gamma \rightarrow A^\vee$ . View  $f_1 \in \text{Hom}(J_\Gamma, A)$  and  $f_2 \in \text{Hom}(J_\Gamma, A^\vee)$ . Denote

$$(f_1, f_2)_\Gamma := f_1 \circ f_2^\vee \in M \xrightarrow{\iota} \mathbb{C}$$

where  $f_2^\vee : A \rightarrow J_\Gamma$  is the dual of  $f_2$  composed with the canonical isomorphism  $J_\Gamma^\vee \cong J_\Gamma$ . If  $A$  is an elliptic curve and identify  $A^\vee$  with  $A$  canonically, then for any morphism  $f : X_\Gamma \rightarrow A$ , we have  $(f, f)_\Gamma = \deg f$ , the degree of  $f$ . Let

$$P_\chi(f_1) = \sum_{\sigma \in \text{Gal}(H_c/K)} f_1(P)^\sigma \chi(\sigma) \in A(H_c)_\mathbb{C} := A(H_c)_\mathbb{Q} \otimes_{(M, \iota)} \mathbb{C}.$$

Similarly, define  $P_{\chi^{-1}}(f_2) \in A^\vee(H_c)_\mathbb{C}$ .

The usual theory of Néron-Tate height over  $K$  gives a  $\mathbb{Q}$ -bilinear non-degenerated pairing (See also [33], §7.1.1)

$$\langle \cdot, \cdot \rangle_K : A(\bar{K})_\mathbb{Q} \times A^\vee(\bar{K})_\mathbb{Q} \longrightarrow \mathbb{R}.$$

The field  $M$  acts on  $A(\bar{K})_\mathbb{Q}$  by definition, and acts on  $A^\vee(\bar{K})_\mathbb{Q}$  through the duality. By the adjoint property of the height pairing, the Neron-Tate height pairing  $\langle \cdot, \cdot \rangle_K$  descends to a  $\mathbb{Q}$ -linear map

$$\langle \cdot, \cdot \rangle_K : A(\bar{K})_\mathbb{Q} \otimes_M A^\vee(\bar{K})_\mathbb{Q} \longrightarrow \mathbb{R}.$$

Denote by  $V$  the  $M$ -module  $A(\bar{K})_\mathbb{Q} \otimes_M A^\vee(\bar{K})_\mathbb{Q}$  for short. The  $\mathbb{Q}$ -linear map  $\langle \cdot, \cdot \rangle_K : V \rightarrow \mathbb{R}$  induces a  $\mathbb{C}$ -linear map  $V \otimes_\mathbb{Q} \mathbb{C} \rightarrow \mathbb{C}$ . Note that

$$V \otimes_\mathbb{Q} \mathbb{C} = V \otimes_M (M \otimes_\mathbb{Q} \mathbb{C}) = \bigoplus_{\iota' : M \hookrightarrow \mathbb{C}} V \otimes_{(M, \iota')} \mathbb{C}$$

where  $\iota'$  runs over all the embeddings from  $M$  to  $\mathbb{C}$ . The above  $\mathbb{C}$ -linear map induces a  $\mathbb{C}$ -linear map  $V \otimes_{(M, \iota)} \mathbb{C} \rightarrow \mathbb{C}$  which gives an  $M$ -linear map  $V \rightarrow \mathbb{C}$  with  $M$  acting on  $\mathbb{C}$  via  $\iota$ . This further induces the following  $M$ -linear map with the action of  $M$  on  $\mathbb{C}$  given by  $\iota$

$$\langle \cdot, \cdot \rangle_K : A(\bar{K})_\mathbb{C} \otimes_M A^\vee(\bar{K})_\mathbb{C} \longrightarrow \mathbb{C}$$

where  $A(\bar{K})_\mathbb{C} := A(\bar{K})_\mathbb{Q} \otimes_{(M, \iota)} \mathbb{C}$  and  $A^\vee(\bar{K})_\mathbb{C} := A^\vee(\bar{K})_\mathbb{Q} \otimes_{(M, \iota)} \mathbb{C}$ .

**Theorem 1.6.** *Under assumptions (1) and (2) above, we have the following identity*

$$L'(1, \phi, \chi) = 2^{-\mu(N, D)} \cdot \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \frac{\langle P_\chi(f_1), P_{\chi^{-1}}(f_2) \rangle_K}{(f_1, f_2)_\Gamma}.$$

Here,  $\mu(N, D)$  is the number of common prime factors of  $N$  and  $D$ ,  $u = [\mathcal{O}_c^\times : \mathbb{Z}^\times]$  and

$$(\phi, \phi)_{\Gamma_0(N)} = \iint_{\Gamma_0(N) \backslash \mathcal{H}} |\phi(x + iy)|^2 dx dy.$$

However, for cube sum problem, the assumption  $(c, N) = 1$  does not hold and we need to carefully choose the test vector  $f$  at any place  $p|(c, N)$ . Based on the work of Yuan-Zhang-Zhang [33], this is in fact a problem of harmonic analysis on local  $p$ -adic representations. Let  $B$  be a quaternion algebra over  $\mathbb{Q}_p$  for some  $p$  with a quadratic sub  $\mathbb{Q}_p$ -algebra, say  $K$ . Denote by  $G = B^\times$ . Let  $\pi$  be an irreducible smooth unitary representation on  $G$  which is of infinite dimension if  $B$  is split. Assume that the central character of  $\pi$  is trivial. Let  $\chi$  be a character on  $K^\times$  such that  $\chi|_{\mathbb{Q}_p^\times} = 1$ . Consider the functional space

$$\mathcal{P}(\pi, \chi) := \text{Hom}_{K^\times}(\pi, \chi^{-1}).$$

In general, its dimension is less than one and here we assume the dimension is one. A nonzero vector  $f \in \pi$  is called a *test vector* for the pair  $(\pi, \chi)$  provided that  $\ell(f) \neq 0$  for any nonzero functional  $\ell \in \mathcal{P}(\pi, \chi)$ . For a nonzero  $f \in \pi$ , consider the following toric integral

$$\beta^0(f) = \int_{\mathbb{Q}_p^\times \backslash K^\times} \frac{(\pi(t)f, f)}{(f, f)} \chi(t) dt$$

where  $(\cdot, \cdot)$  is any nonzero invariant Hermitian pairing on  $\pi$  and  $dt$  is any Haar measure on  $\mathbb{Q}_p^\times \backslash K^\times$ . This integral is absolutely convergent. Moreover,  $f$  is a test vector for  $(\pi, \chi)$  if and only if  $\beta^0(f) \neq 0$ .

Denote by  $n$  the conductor of  $\pi$ , that is, the minimal non-negative integer such that the invariant subspace of  $\pi$  under  $U_0(n)$  is nonzero. Here  $U_0(n) = R_0(n)^\times$  with  $R_0(n) = \begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^n \mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ . Denote by  $c$  the conductor of  $\chi$ , that is, the minimal non-negative integer such that  $\chi$  is trivial on the units of  $\mathcal{O}_c := \mathbb{Z}_p + p^c \mathcal{O}_K$ .

Assume  $K$  is split or  $c$  is large enough. In this case, as the functional space  $\mathcal{P}(\pi, \chi)$  is nonzero, the quaternion  $B$  must be split and we shall take the test vector as the new vector of  $\pi$ . Precisely, the test vector  $f$  is a nonzero vector in the line of  $\pi$  consisting with invariant vectors under the actions of  $R^\times$  where  $R$  is an Eichler order of discriminant  $n$  such that  $R \cap K = \mathcal{O}_c$ . By definition, all such orders are  $\text{GL}_2(\mathbb{Q}_p)$ -conjugate to the order  $R_0(n)$ . Note that the toric integral is invariant by modifying  $f$  to  $\pi(t)f$  for any  $t \in K^\times$ . Thus, what matters here is the  $K^\times$ -conjugacy classes of such Eichler orders. In general, the set of  $K^\times$ -conjugacy classes of such Eichler orders is finite but not a singleton (See also [3], Lemma 3.2). Here, we shall take the Eichler order  $R$  to be *admissible* for the pair  $(\pi, \chi)$ . This means that it is the intersection of two maximal orders  $R'$  and  $R''$  of  $M_2(\mathbb{Q}_p)$  such that  $R' \cap K = \mathcal{O}_c$  and

$$R'' \cap K = \begin{cases} \mathcal{O}_{c-n}, & \text{if } c \geq n; \\ \mathcal{O}_K, & \text{otherwise.} \end{cases}$$

Such order exists if and only if the following condition holds:

$$(*) \quad c - n + e - 1 \geq 0 \text{ if } K \text{ is nonsplit}$$

where  $e$  is the ramification index of  $K/\mathbb{Q}_p$ . If exists, it is unique up to conjugation by normalizers of  $K^\times$  in  $\text{GL}_2(\mathbb{Q}_p)$ . Moreover, it is even unique up to  $K^\times$ -conjugation unless  $K$  is split and  $0 < c < n$ . Finally, using Kirillov model of  $\pi$ , we can prove that the toric integral  $\beta^0(f)$  is nonvanishing for any nonzero  $f \in \pi$  invariant under the actions of  $R^\times$  with  $R$  an admissible order for  $(\pi, \chi)$  (See also [3] Proposition 3.12 and Lemma 3.2 in this paper).

Globally, write  $N = N_0 N_1$  with  $N_0 = \prod_{p|(N, c)} p^{\text{ord}_p(N)}$  the  $c$ -part of  $N$ . In particular,  $(N_1, c) = 1$ . Assume:

- The condition (1) and (2) hold for  $N_1$  and  $c$ : if  $p|(N_1, D)$  then  $\text{ord}_p(N_1) = 1$  and the set  $\Sigma$  has even cardinality, where  $\Sigma$  consists of prime factors  $p$  of  $N_1$  satisfying
  - either  $p$  is inert in  $K$  and  $\text{ord}_p(N_1)$  is odd,
  - or  $p$  is ramified in  $K$  and  $\chi([\mathfrak{p}]) = a_p$  where  $[\mathfrak{p}] \in \text{Pic}(\mathcal{O}_c)$  is the ideal class of the prime ideal  $\mathfrak{p}$  above  $p$ .

- The condition  $(*)$  holds for the  $N_0$ -part:  $\text{ord}_p(c) - \text{ord}_p(N) + e_p - 1 \geq 0$  if  $p|N_0$  and  $K_p$  is nonsplit.

This condition implies that the root number  $\epsilon(\phi, \chi)$  is  $-1$  (See also Lemma 3.1). Let  $B$  be the indefinite quaternion algebra over  $\mathbb{Q}$  ramified exactly at places in  $\Sigma$ . Fix an embedding from  $K$  to  $B$ . Let  $R$  be an order of  $B$  with discriminant  $N$  such that  $R \cap K = \mathcal{O}_c$  and  $R_p$  is admissible for  $(\phi, \chi)$  for any prime  $p|N_0$ . As before, denote by  $\Gamma := \{\gamma \in R^\times | N_B(\gamma) = 1\}$  and  $X_\Gamma$  is the Shimura curve over  $\mathbb{Q}$  with level  $\Gamma$ . There exists an admissible modular parametrization  $f_1 : X_\Gamma \rightarrow A$  which is unique in the sense as before. Let  $P \in X_\Gamma(H_c)$  be the point represented by the point in  $\mathcal{H}$  fixed by  $K^\times$ . Let

$$P_\chi(f_1) = \sum_{\sigma \in \text{Gal}(H_c/K)} f_1(P)^\sigma \chi(\sigma) \in A(H_c)_\mathbb{C}.$$

Similarly, there is an admissible modular parametrization  $f_2 : X_\Gamma \rightarrow A^\vee$  and one may define  $P_{\chi^{-1}}(f_2) \in A^\vee(H_c)_\mathbb{C}$ .

**Theorem 1.7.** *Assume conditions in (1) and (2) hold for  $N_1$  and  $c$  while  $(*)$  holds for the  $N_0$ -part, we have the following identity*

$$L'^{(S)}(1, \phi, \chi) = 2^{-\mu(N_1, D)} \cdot \frac{8\pi^2(\phi, \phi)_{\Gamma_0(N)}}{u^2 \sqrt{|Dc^2|}} \cdot \frac{\langle P_\chi(f_1), P_{\chi^{-1}}(f_2) \rangle_K}{(f_1, f_2)_\Gamma}.$$

Here  $\mu(N_1, D)$  is the number of common prime factors of  $N_1$  and  $D$ , the set

$$S = \{p|(N, Dc) \mid \text{if } p||N \text{ then } \text{ord}_p(c/N) \geq 0\}$$

and  $L^{(S)}(s, \phi, \chi)$  is obtained by the  $L$ -function  $L(s, \phi, \chi)$  with Euler factors at places in  $S$  removed, and other terms are the same as in Theorem 1.6.

This is a special case of Theorem 3.5. The difference between the above construction of Heegner point and the one in [3] is at those places  $p|N_0$  ramified in  $K$  such that  $\text{ord}_p(c) + 1 = \text{ord}_p(N)$ . At these places, we require here that  $f$  is of  $\Gamma_0(N)$ -level structure while in [3], it is considered to be  $\chi^{-1}$ -eigen. A more general construction for abelian varieties over totally real fields is considered. In particular, an explicit Gross-Zagier (see also Theorem 3.5) is obtained as an application of the variant of Gross-Zagier formula in [3] Theorem 1.6.

Next, we explain how to prove Theorem 1.1 and 1.2. Let  $E/\mathbb{Q}$  be the elliptic curve with Weierstrass equation  $y^2 = x^3 + 1$ . The elliptic curve  $E$  is isomorphic to the modular curve  $X_0(36)$  over  $\mathbb{Q}$ . Let  $K \subset \mathbb{C}$  be the imaginary quadratic field over  $\mathbb{Q}$  generated by  $\omega = e^{2\pi i/3}$  and  $\mathcal{O}_K$  its ring of integers. It is known that  $E$  is endowed with complex multiplication  $[\ ] : \mathcal{O}_K \simeq \text{End}_\mathbb{C}(E)$ . For any  $n \in \mathbb{Q}^\times$ , let  $E^{(n)}/\mathbb{Q}$  be the elliptic curve  $y^2 = x^3 + n^2$ . Then  $E^{(n)}$  is isogenous to  $C^{(n)}$  over  $\mathbb{Q}$  and  $\text{rank}_{\mathcal{O}_K} E^{(n)}(K) = \text{rank}_\mathbb{Z} E^{(n)}(\mathbb{Q})$ . Thus  $2n$  is a cube sum if and only if  $E^{(n)}(K)$  has a point of infinite order.

Let  $k \geq 1$  be an integer. Let  $p_1, p_2, \dots, p_k$  be distinct odd primes  $\equiv 2, 5 \pmod{9}$ . Let  $n = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_k^{\epsilon_k}$  with  $\epsilon_i = \pm 1$  and let  $N = p_1 p_2 \dots p_k$ . Let  $\chi_n : \text{Gal}(K^{\text{ab}}/K) \rightarrow \mathbb{C}^\times$  be the character such that  $\chi_n(\sigma) = (\sqrt[3]{n})^{\sigma-1}$ ,  $\forall \sigma \in \text{Gal}(K^{\text{ab}}/K)$ . Then  $c(\chi) = 3N$ . Denote by  $E(K(\sqrt[3]{n}))^{\chi_n}$  the subgroup of  $E(K(\sqrt[3]{n}))$  consisting of points  $P$  such that  $P^\sigma = [\chi_n(\sigma)]P$  for any  $\sigma \in \text{Gal}(K(\sqrt[3]{n})/K)$ . The group  $E^{(n)}(K)$  is isomorphic to  $E(K(\sqrt[3]{n}))^{\chi_n}$  under the map  $\phi : E^{(n)} \rightarrow E$  given as  $(x, y) \mapsto \left(-\frac{\sqrt[3]{n}x}{n}, \frac{y}{n}\right)$ .

Thus  $2n$  is a cube sum if and only if there is a point in  $E(K(\sqrt[3]{n}))^{\chi_n}$  with infinite order.

The indefinite quaternion algebra  $B$  determined by  $E$  and  $\chi_n$  as above is  $M_2(\mathbb{Q})$ . We carefully take an embedding  $\rho : K \hookrightarrow B$  such that  $R_0(36) \cap K = \mathcal{O}_{6N}$  with  $R_0(36) = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 36\mathbb{Z} & \mathbb{Z} \end{pmatrix}$  and  $R_0(36)$  is admissible for  $(E, \chi_n)$  at the place 3. A concrete such embedding is given before Theorem 2.5. Let  $f : X_0(36) \rightarrow E$  be the modular parametrization of degree one mapping the cusp  $[\infty]$  to the identity  $O$  on  $E$ . Then  $f$  is essentially a test vector described as above in this special situation (See also Lemma 3.7).

The  $L$ -function  $L(s, E, \chi_n)$  satisfies  $L(s, E, \chi_n) = L(s, E^{(n)})L(s, E^{(n^{-1})})$ . Assume  $k$  is odd. Then the condition  $\sum_1^k \epsilon_i \equiv 1 \pmod{3}$  is equivalent to  $\epsilon(E, \chi_n) = \epsilon(E^{(n)}) = -1$ . Let  $\Omega^{(n)}$  denote the minimal real period of  $E^{(n)}$  and  $\Omega$  the one of  $E$ . Let  $P_0$  be the CM point on  $X_0(36)$  represented by the fixed point on  $\mathcal{H}$  of  $K^\times$  under our choice of embedding. Then  $P_0$  is defined over  $H_{6N}$ . Applying Theorem 1.7 to  $E, \chi_n$  and  $f$ , we have the following height formula.

**Corollary 1.8.** *Let  $k$  be an odd integer. Suppose  $p_1, p_2, \dots, p_k$  are distinct odd prime numbers  $\equiv 2, 5 \pmod{9}$ . Let  $n = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_k^{\epsilon_k}$  with  $\epsilon_i = \pm 1$  and  $\sum \epsilon_i \equiv 1 \pmod{3}$ . The Heegner divisor*

$$z_n := \sum_{\sigma \in \text{Gal}(H_{6N}/K)} [\chi_n^{-1}(\sigma)] f(P_0)^\sigma \in E(K(\sqrt[3]{n}))^{\chi_n}$$

*satisfies the following Gross-Zagier formula:*

$$L'(1, E^{(n)}) L(1, E^{(n^{-1})}) = 3^{-3} \cdot \Omega^{(n)} \Omega^{(n^{-1})} \cdot \hat{h}_{\mathbb{Q}}(z_n),$$

*where  $\hat{h}_{\mathbb{Q}}$  is the canonical Néron -Tate height on  $E(\bar{\mathbb{Q}})$  over  $\mathbb{Q}$ .*

From this height formula, we see that the Heegner point  $z_n$  is of infinite order if and only if the  $L$ -function  $L(s, E, \chi_n)$  has vanishing order 1 at  $s = 1$ . Recall when  $k = 1$ ,  $\dim_{\mathbb{F}_3} \text{Sel}_3(E^{(p^*)})/E^{(p^*)}(\mathbb{Q})_{\text{tor}} \leq 1$  and  $\dim_{\mathbb{F}_3} \text{Sel}_3(E^{(p^{*-1})})/E^{(p^{*-1})}(\mathbb{Q})_{\text{tor}} = 0$ . The Birch and Swinnerton-Dyer conjecture predicts that

$$\text{ord}_{s=1} L(s, E^{(p^*)}) = \text{rank}_{\mathbb{Z}} E^{(p^*)}(\mathbb{Q}) = 1 \text{ and } \text{ord}_{s=1} L(s, E^{(p^{*-1})}) = \text{rank}_{\mathbb{Z}} E^{(p^{*-1})}(\mathbb{Q}) = 0.$$

We will prove this by showing that the Heegner point  $z_{p^*}$  is of infinite order.

Next we explain how to prove the nontriviality of Heegner points in general. For any  $d = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_k^{\epsilon_k}$  with  $\epsilon_i = 0, \pm 1$ , let  $\chi_d : \text{Gal}(H_{6N}/K) \rightarrow \mathbb{C}^\times$  be the character such that  $\chi_d(\sigma) = (\sqrt[3]{d})^{\sigma-1}$ ,  $\forall \sigma \in \text{Gal}(H_{6N}/K)$ . Define the Heegner divisor

$$z_d := \sum_{\sigma \in \text{Gal}(H_{6N}/K)} [\chi_d^{-1}(\sigma)] f(P_0)^\sigma \in E(K(\sqrt[3]{d}))^{\chi_d}.$$

Summing over all these Heegner divisors, we have an identity:

$$\sum_d z_d = 3^k z_0,$$

where  $z_0 = \text{Tr}_{H_{6N}/H_0} f(P_0) \in E(H_0)$  is the genus Heegner point and  $H_0 = K(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \dots, \sqrt[3]{p_k}) \subset H_{3N}$  is the genus field over  $K$ . By a similar argument due to Heegner (see also Birch as in [1], and Satge in [23]), it follows from the key fact  $3 \nmid [H_{3N} : H_0]$  that the genus Heegner point  $z_0$  is of infinite order. Then we examine which Heegner points will contribute on the left hand side of the equality. By Euler system property of Heegner divisors, for any  $d = p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_k^{\epsilon_k}$  with some  $\epsilon_i = 0$ , the Heegner divisor  $z_d$  is zero. Thus only Heegner points  $z_d$  with  $\epsilon_i \neq 0, \forall i$ , remain and at least one such Heegner point is of infinite order and Theorem 1.1 follows. Note that if  $k = 1$ , there is exactly one term remains on the left hand side and the first part of Theorem 1.2 follows. Comparing the height formula in Corollary 1.8 and BSD conjecture, the 3-part of the second assertion in Theorem 1.2 follows from the 3-divisibility of the Heegner point  $z_n$  in  $E(K(\sqrt[3]{n}))^{\chi_n}$ . The  $\ell$ -part of the second assertion in Theorem 1.2,  $\ell \nmid 6p$ , follows from work of Kolyvagin [14], Perrin-Riou [20] and Kobayashi [13]

## 2. NONTRIVIALITY OF HEEGNER POINTS

Recall the elliptic curve  $E/\mathbb{Q}$  is given by the Weierstrass equation  $y^2 = x^3 + 1$  and the complex multiplication is fixed by the isomorphism  $[\ ] : \mathcal{O}_K \rightarrow \text{End}_{\mathbb{C}}(E)$  such that  $[\omega](x, y) = (\omega x, y)$ .

**Proposition 2.1.** *The group of rational points  $E(\mathbb{Q})$  is torsion cyclic of order 6 and is generated by the point  $(2, 3)$ . The group of  $K$ -points  $E(K)$  is torsion and equal to  $E[2\sqrt{-3}]$ .*

*Proof.* Let  $m$  be an integer such that  $[m]E(\mathbb{Q})_{\text{tor}} = 0$ . For any prime number  $p \nmid 6m$ ,  $E(\mathbb{Q})_{\text{tor}} \subset E(\mathbb{Q}_p)[m] \simeq E(\mathbb{F}_p)[m]$  under reduction mod  $p$ . When  $p \equiv 5 \pmod{6}$ , the reduction of  $E$  mod  $p$  is supersingular, and then  $E(\mathbb{F}_p) = p + 1$ . Thus  $\#E(\mathbb{Q})_{\text{tor}} \mid 6$ . On the other hand, the point  $(2, 3)$  is a rational point of order 6. So  $E(\mathbb{Q})_{\text{tor}}$  is cyclic of order 6 and generated by  $(2, 3)$ . There is a rational 2-torsion point  $(-1, 0)$  on  $E$  and, using the 2-descent method, one can show  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/\mathbb{Q})/E[2](\mathbb{Q}) = 0$  and hence  $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ .

For any point  $P \in E(K)$ ,  $P + \bar{P}$  is a rational point and  $[6](P + \bar{P}) = 0$ . If  $[6]P \neq O$ , then it has coordinates of form  $(x, y\sqrt{-3})$  with  $x, y \in \mathbb{Q}$  and so does  $[6\omega]P = (\omega x, y\sqrt{-3})$ . But this forces  $x = 0$  which is impossible. So  $E(K)$  is torsion.

The conductor of the Hecke character associated to the elliptic curve  $E/K$  is the ideal  $(2\sqrt{-3})$ . By the main theorem of the complex multiplication,  $E(K) \subset E[2\sqrt{-3}]$ . On the other hand, there are exactly 12  $K$ -points generated by  $E(\mathbb{Q})$  under complex multiplication by  $\mathcal{O}_K$ , namely,  $O, (-\omega^n, 0), (0, \pm 1), (2\omega^n, 3), (2\omega^n, -3)$  with  $n = 0, 1, 2$ . So  $E(K)_{\text{tor}} = E[2\sqrt{-3}]$ .  $\square$



Let  $U_0(36)$  be the open subgroup of  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$  consisting of matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  such that  $c \equiv 0 \pmod{36}$ . Let  $\Gamma_0(36) = \mathrm{GL}_2(\mathbb{Q})^+ \cap U_0(36)$ . Then  $X_0(36)$  is the modular curve over  $\mathbb{Q}$  whose underlying Riemann surface is

$$X_0(36)(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})^+ \backslash (\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})) \times \mathrm{GL}_2(\mathbb{A}_f) / U_0(36) \simeq \Gamma_0(36) \backslash \mathcal{H} \bigsqcup \Gamma_0(36) \backslash \mathbb{P}^1(\mathbb{Q}).$$

Elements in  $S = \Gamma_0(36) \backslash \mathbb{P}^1(\mathbb{Q})$  are called cusps of  $X_0(36)$  and there are 12 cusps, 6 among which are rational and the other 6 are defined over the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-3})$ . For each  $z \in \mathbb{P}^1(\mathbb{Q})$ , denote by  $[z]$  the cusp on  $X_0(36)$  represented by  $z$ . The modular curve  $X_0(36)$  is a projective smooth curve of genus 1 over  $\mathbb{Q}$  with a rational cusp  $[\infty]$  and we have an elliptic curve  $(X_0(36), [\infty])$  over  $\mathbb{Q}$  with  $[\infty]$  as its zero element.

For any field extension  $F/\mathbb{Q}$ , we write  $\mathrm{Isom}_F(X_0(36))$  for the group of algebraic isomorphisms of  $X_0(36)$  defined over  $F$ , and  $\mathrm{Aut}_F(X_0(36))$  for the subgroup of algebraic isomorphisms over  $F$  which fix the cusp  $[\infty]$ . Define  $N$  to be the normalizer of  $\Gamma_0(36)$  in  $\mathrm{GL}_2^+(\mathbb{Q})$ . The action of  $N$  on  $X_0(36)$  induces an injective homomorphism

$$T : N/\mathbb{Q}^\times \Gamma_0(36) \rightarrow \mathrm{Isom}_{\mathbb{C}}(X_0(36)) = \mathrm{Aut}_{\mathbb{C}}(X_0(36)) \ltimes X_0(36)(\mathbb{C}).$$

**Proposition 2.2.** *The elliptic curve  $(X_0(36), [\infty])$  has complex multiplication by  $\mathcal{O}_K$  and Weierstrass equation  $y^2 = x^3 + 1$  such that the cusp  $[0]$  has coordinates  $(2, 3)$ .*

We identify the elliptic curve  $(X_0(36), [\infty])$  with  $E$  and then  $E(K) = S$ .

*Proof.* There are two special linear fractional transformations  $X_0(36)$  given by matrices

$$A = \begin{pmatrix} 1 & 1/6 \\ 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 \\ -36 & 0 \end{pmatrix}.$$

Since the transformation  $T(A)$  is of order 6 and fixes  $[\infty]$ ,  $T(A)$  acts on the elliptic curve  $(X_0(36), [\infty])$  as a complex multiplication by a primitive sixth root of unity. Thus the elliptic curve  $(X_0(36), [\infty])$  has complex multiplication by  $\mathcal{O}_K$ . The linear fractional transformation  $T(B)$  is the Atkin-Lehner involution on  $X_0(36)$ , which is rational of order 2.

For  $\epsilon \in \mathrm{Aut}_{\mathbb{C}}(X_0(36)) = \mathcal{O}_K^\times$  and  $\alpha \in X_0(36)(\mathbb{C})$ , denote  $t_{\epsilon, \alpha}$  to be the isomorphism  $P \mapsto [\epsilon]P + \alpha$  in  $\mathrm{Aut}_{\mathbb{C}}(X_0(36)) \ltimes X_0(36)(\mathbb{C})$ . We simply write  $t_{1, \alpha}$  as  $t_\alpha$ , and  $t_{\epsilon, [\infty]}$  as  $[\epsilon]$ . Note  $t_{\epsilon, \alpha}^2 = t_{\epsilon^2, [\epsilon]\alpha + \alpha}$  for any  $\epsilon \in \mathcal{O}_K^\times$  and  $\alpha \in X_0(36)(\mathbb{C})$ . Since  $T(B)$  is rational of order 2, it is either  $t_{-1, \alpha}$  for some rational  $\alpha$ , or  $t_\alpha$  for some rational point  $\alpha$  of order 2. Note  $T(B)$  fixes the point  $[\sqrt{-1}/6]$  and then  $T(B) = t_{-1, \alpha}$  for some rational  $\alpha$ . Since  $t_\alpha = t_{-1, \alpha} \circ [-1] = T(BA^3)$  and the matrix

$$BA^3 = \begin{pmatrix} 0 & 1 \\ -36 & -18 \end{pmatrix}$$

is of order 6 in  $\Phi$  and takes cusp  $[\infty]$  to cusp  $[0]$ , the cusp  $[0]$  is rational of order 6 and the Atkin-Lehner involution  $T(B) = t_{-1, [0]}$ .

It is known that every elliptic curve over  $\mathbb{Q}$  is parametrized by the modular curve of the same level as its conductor. It follows that  $(X_0(36), [\infty])$  is isogenous to the elliptic curve  $E : y^2 = x^3 + 1$ . However, there are exactly 4 isomorphism classes of elliptic curves over  $\mathbb{Q}$  with conductor 36 and the elliptic curve  $y^2 = x^3 + 1$  is the unique one with a rational point of order 6 and with complex multiplication by  $\mathcal{O}_K$ . So  $(X_0(36), [\infty])$  is isomorphic to the elliptic curve  $E : y^2 = x^3 + 1$ . The rational points of order 6 on  $y^2 = x^3 + 1$  are  $(2, \pm 3)$ . This isomorphism is unique if it maps  $[0]$  to  $(2, 3)$ . Thus  $E$  has a Weierstrass equation  $y^2 = x^3 + 1$  with  $(2, 3)$  as the coordinates of the cusp  $[0]$ .  $\square$

Let  $\phi = \sum_{n \geq 1} a_n q^n$  be the unique new form of level  $\Gamma_0(36)$  and weight 2. Then the Néron differential on  $X_0(36)$  is  $dx/2y = \phi(q)dq/q$ . At  $[\infty]$ , it is represented by  $dq$  and  $T(A)^*(dq) = -\omega^2 dq$ . On the other hand,  $[-\omega^2](x, y) = (\omega^2, -y)$  and then  $[-\omega^2]^*(dx/2y) = -\omega^2 dx/2y$ . So we have  $T(A) = [-\omega^2]$ .

**Proposition 2.3.** *The natural homomorphism  $T$  induces an isomorphism*

$$N/\mathbb{Q}^\times \Gamma_0(36) \simeq \mathrm{Isom}_K(E) = \mathrm{Aut}_K(E) \ltimes E(K).$$

More precisely, one has the following relations:

$$\begin{aligned}
t_O &= T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & t_{(0,1)} &= T \begin{pmatrix} -2 & -1 \\ 36 & 16 \end{pmatrix}, & t_{(0,-1)} &= T \begin{pmatrix} 16 & 1 \\ -36 & -2 \end{pmatrix}, \\
t_{(-1,0)} &= T \begin{pmatrix} 9 & 4 \\ -144 & -63 \end{pmatrix}, & t_{(-\omega,0)} &= T \begin{pmatrix} 39 & 4 \\ 144 & 15 \end{pmatrix}, & t_{(-\omega^2,0)} &= T \begin{pmatrix} 87 & -20 \\ 144 & -33 \end{pmatrix}, \\
t_{(2,3)} &= T \begin{pmatrix} 0 & 1 \\ -36 & -18 \end{pmatrix}, & t_{(2\omega,3)} &= T \begin{pmatrix} 12 & 1 \\ 36 & 6 \end{pmatrix}, & t_{(2\omega^2,3)} &= T \begin{pmatrix} 12 & 11 \\ -36 & -30 \end{pmatrix}, \\
t_{(2,-3)} &= T \begin{pmatrix} -18 & -1 \\ 36 & 0 \end{pmatrix}, & t_{(2\omega,-3)} &= T \begin{pmatrix} -6 & 1 \\ 36 & -12 \end{pmatrix}, & t_{(2\omega^2,-3)} &= T \begin{pmatrix} 6 & 1 \\ 36 & 12 \end{pmatrix}.
\end{aligned}$$

*Proof.* For any  $C \in \mathrm{GL}_2(\mathbb{Q})^+$ , if  $T(C)[\infty] = \alpha \in S = E(K)$ , then  $t_{-\alpha} \circ T(C)$  is an element in  $\mathrm{Aut}_K(E)$ . Thus the image of  $T$  lies in  $\mathrm{Aut}_K(E) \ltimes E(K)$ . Since  $T(A) = [-\omega^2]$ ,  $T(BA^3) = t_{[0]}$  and  $[-\omega^2], t_{[0]}$  generates  $\mathrm{Isom}_K(E)$ , the homomorphism  $T$  is an isomorphism between  $N/\mathbb{Q}^\times \Gamma_0(36)$  and  $\mathrm{Isom}_K(E)$ .

The verification of the relations is straightforward.  $\square$

**Corollary 2.4.** *The complete list of cusps on  $X_0(36)$  is given as follows:*

$$[0], [1/2], [1/3], [-1/3], [-1/16], [1/6], [-1/6], [-4/9], [13/48], [29/48], [-1/18], [\infty].$$

As is seen, we have  $S \simeq E[2\sqrt{-3}]$ . Let

$$\tau : \mathbb{Z}[\omega]/(2\sqrt{-3}) \longrightarrow S$$

be the unique isomorphism such that  $\tau(0) = [\infty]$  and  $\tau(1) = [0]$ . Then we have that

$$\begin{aligned}
\tau(-1) &= [-1/2], & \tau(\omega) &= [1/3], & \tau(\omega^2) &= [-1/3], & \tau(3) &= [-1/16], \\
\tau(-\omega) &= [-1/6], & \tau(-\omega^2) &= [1/6], & \tau(4) &= [-4/9], & \tau(3\omega) &= [13/48], \\
\tau(3\omega^2) &= [29/48], & \tau(2) &= [-1/18].
\end{aligned}$$

Let  $U \subset U_0(36)$  be the subgroup of index 2 consisting of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } a \equiv d \pmod{3}.$$

Let  $X_U$  be the modular curve over  $\mathbb{Q}$  whose underlying Riemann surface is

$$X_U(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})^+ \backslash (\mathcal{H} \sqcup \mathbb{P}^1(\mathbb{Q})) \times \mathrm{GL}_2(\mathbb{A}_f)/U.$$

Under class field theory,  $\mathbb{A}_f^\times/\mathbb{Q}^\times \det(U) \simeq \mathrm{Gal}(K/\mathbb{Q})$ . By noting that  $\mathrm{GL}_2(\mathbb{Q})^+ \cap U = \Gamma_0(36)$ , we see that the modular curve  $X_U$  is isomorphic to  $X_0(36) \times_{\mathbb{Q}} K$  as a curve over  $\mathbb{Q}$ . Let  $U_0(36)/U = \langle \epsilon \rangle$  where

$$\epsilon = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The non-trivial Galois action of  $\mathrm{Gal}(K/\mathbb{Q})$  on  $X_U$  is given by the right-translation of  $\epsilon$  on  $X_U$ . We have

$$\mathrm{Isom}_{\mathbb{Q}}(X_U) = (\mathbb{Z}[\omega]/(2\sqrt{-3}) \rtimes \mathcal{O}_K^\times) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

Let  $N_{\mathrm{GL}_2(\mathbb{A}_f)}(U)$  be the normalizer of  $U$  in  $\mathrm{GL}_2(\mathbb{A}_f)$ . Then there is a natural homomorphism  $N_{\mathrm{GL}_2(\mathbb{A}_f)}(U) \longrightarrow \mathrm{Isom}_{\mathbb{Q}}(X_U)$  induced by right translation on  $X_U$ . The curve  $X_U$  is not geometrically connected and has two connected components over  $\mathbb{C}$ . An element  $g \in N_{\mathrm{GL}_2(\mathbb{A}_f)}(U)$  maps one component of  $X_U$  onto another if and only if it has image  $-1$  under the composition of the following morphisms:

$$\mathrm{GL}_2(\mathbb{A}_f) = \mathrm{GL}_2(\mathbb{Q})^+ U_0(32) \xrightarrow{\det} \mathbb{Q}_+^\times \widehat{\mathbb{Z}}^\times \longrightarrow \mathbb{Z}_3^\times / (1 + 3\mathbb{Z}_3),$$

where the last morphism is the projection from  $\widehat{\mathbb{Z}}^\times$  to its 3-adic factor.

Let  $k \geq 1$  be an odd integer. Let  $p_1, p_2, \dots, p_k$  be distinct odd primes  $\equiv 2, 5 \pmod{9}$  and  $N = p_1 p_2 \cdots p_k$ . Let  $\rho : K \rightarrow M_2(\mathbb{Q})$  be the normalized embedding given by

$$\omega \mapsto \begin{pmatrix} 4 & -\frac{7N}{6} \\ \frac{18}{N} & -5 \end{pmatrix}$$

with fixed point  $h_0 = \left(1 + \frac{\sqrt{-3}}{9}\right) \frac{N}{4} \in \mathcal{H}$ . Then  $\widehat{K}^\times \cap U = \widehat{\mathcal{O}}_{6N}^\times$ . Let  $w = \begin{pmatrix} 1 & -\frac{N}{2} \\ 0 & -1 \end{pmatrix}$  be an element in  $N_{\mathrm{GL}_2(\mathbb{Q})^+}(K^\times)$  which normalises  $U$  and hence induces an isomorphism in  $\mathrm{Isom}_{\mathbb{Q}}(X_U)$ . The groups



$K_2^\times/\mathbb{Q}_2^\times(1+2\mathcal{O}_2) = \langle \omega_2 \rangle^{\mathbb{Z}/3\mathbb{Z}}$  and  $\mathcal{O}_3^\times/\mathbb{Z}_3^\times(1+3\mathcal{O}_3) = \langle \omega_3 \rangle^{\mathbb{Z}/3\mathbb{Z}}$ . By noting that  $\omega_2$  and  $\omega_3$  normalises  $U$  in  $\mathrm{GL}_2(\mathbb{A}_f)$ , we have natural homomorphisms

$$K_2^\times/\mathbb{Q}_2^\times(1+2\mathcal{O}_2) \rightarrow \mathrm{Isom}_{\mathbb{Q}}(X_U) \text{ and } \mathcal{O}_3^\times/\mathbb{Z}_3^\times(1+3\mathcal{O}_3) \rightarrow \mathrm{Isom}_{\mathbb{Q}}(X_U).$$

**Theorem 2.5.** *For any point  $P \in X_U$ ,*

$$P^{\omega_2} = P + \tau(2), P^{\omega_3} = [\omega]P, P^{w\epsilon} = [-1]P.$$

*Proof.* Since  $\det \omega_2 = 1, \det \omega_3 = 1$  and  $\det w\epsilon = 1$ , there exist  $\alpha, \beta, \gamma \in \mathcal{O}_K^\times$  and  $R, S, T \in E(K)$  such that, for all  $P \in X_U$ ,

$$P^{\omega_2} = [\alpha]P + R, P^{\omega_3} = [\beta]P + S, \text{ and } P^{w\epsilon} = [\gamma]P + T.$$

Note

$$\begin{pmatrix} 1 & 2^{-1} \\ 18 & 10 \end{pmatrix} \omega_2 \in U \quad \text{and} \quad \begin{pmatrix} 1 & 3^{-1} \\ 36 & 13 \end{pmatrix} \omega_3 \in U, \begin{pmatrix} 1 & \frac{N}{2} \\ 0 & 1 \end{pmatrix} w\epsilon \in U.$$

Taking  $P = [\infty]$ ,

$$R = [\infty]^{\omega_2} = [1/18], S = [\infty]^{\omega_3} = [1/36], T = [\infty]^{w\epsilon} = [\infty].$$

Taking  $P = [0]$ ,

$$[\alpha][0] + [1/18] = [1/20], [\beta][0] = [1/39], [\gamma][0] = [N/2].$$

When identified with identities in  $\mathcal{O}_K/(2\sqrt{-3})$ , it follows that  $\alpha = 1, \beta = \omega$  and  $\gamma = -1$ .  $\square$

Let  $P_0 = [h_0, 1]$  be a complex multiplication point in  $X_0(36)$ . By the main theorem of complex multiplication, the point  $P_0$  is in  $E(K^{\mathrm{ab}})$ . Let  $\sigma : K^\times \backslash \widehat{K}^\times \rightarrow G_K^{\mathrm{ab}}$  be the Artin reciprocity law.

**Corollary 2.6.** *The point  $P_0 \in E(H_{6N})$  satisfies*

$$P_0^{\sigma\omega_2} = P_0 + \tau(2), P_0^{\sigma\omega_3} = [\omega]P_0, \overline{P_0} = [-1]P_0.$$

*Proof.* Consider the normalised embedding  $\rho : K \rightarrow M_2(\mathbb{Q})$ . Let  $P = [h_0, 1]$  be a point in  $X_U$ . By Shimura's reciprocity law,  $P^{\sigma t} = [h_0, \rho(t)]$  for any  $t \in \widehat{K}^\times$ . Thus  $P^{\sigma t} = P$  if and only if  $t \in K^\times (U \cap \widehat{K}^\times) = K^\times \widehat{\mathcal{O}}_{6N}^\times$ . Hence  $P \in X_U(H_{6N})$ . In view of Theorem 2.5, by Shimura's reciprocity law, one has

$$P^{\sigma\omega_2} = P + \tau(2), P^{\sigma\omega_3} = [\omega]P, \overline{P} = [-1]P.$$

Since  $P_0$  is the image of  $P$  under the natural projection, the corollary follows.  $\square$

Let  $H_0 = K(\sqrt[3]{p_1}, \sqrt[3]{p_2}, \dots, \sqrt[3]{p_k})$  be the genus field over  $K$ .

**Proposition 2.7.** a. *The field  $H_0$  is contained in  $H_{3N}$  and the Galois group  $\mathrm{Gal}(H_0/K) = \langle \sigma_{\omega_p} \rangle_{p|N}$  and  $\sigma_{\omega_3}(\sqrt[3]{p^*}) = \omega \sqrt[3]{p^*}$  for  $p \mid N$ .*  
b.  *$H_6 = K(\sqrt[3]{2})$  with Galois group  $\mathrm{Gal}(H_6/K) = \langle \sigma_{\omega_2} \rangle$  and  $H_{6N} = H_{3N}(\sqrt[3]{2})$  with  $\mathrm{Gal}(H_{6N}/H_{3N}) = \langle \sigma_{\omega_2} \rangle$  and  $\sigma_{\omega_2}(\sqrt[3]{2}) = \sigma_{\omega_3}^{-1}(\sqrt[3]{2}) = \omega^2 \sqrt[3]{2}$ .*

*Proof.* For  $p \mid N$ , let  $L = K(\sqrt[3]{p})$  and  $H_0$  is the composition field of these cubic extensions  $L$ . The field extension  $L/K$  is totally ramified at the prime ideals  $(\sqrt{-3})$  and  $(p)$ . So the local norm group of  $L$  at  $(\sqrt{-3})$  (resp.  $(p)$ ) cannot contain  $\mathcal{O}_3^\times$  (resp.  $\mathcal{O}_p^\times$ ). We claim that  $\mathbb{Z}_3^\times(1+3\mathcal{O}_3)\mathbb{Z}_p^\times(1+p\mathcal{O}_p)$  fixes  $L$  under the Artin reciprocity law

First we show that  $\mathbb{Z}_p^\times(1+p\mathcal{O}_p)$  fixes  $L$ . Let  $e(X) = -pX + X^{p^2-1}$  be the Lubin-Tate series of  $K_p$  w.r.t. the primitive element  $-p$  and let  $\mathcal{F}$  be the Lubin-Tate  $\mathcal{O}_p$ -module associated to  $e(X)$ . For any element  $\alpha \in \mathcal{O}_p$ , denote the action of  $\alpha$  on  $\mathcal{F}$  as  $[\alpha]_{\mathcal{F}}$ . Then it is easily checked that  $[\omega_p]_{\mathcal{F}}(X) = \omega X$ . Let  $K_p^1$  be the first Lubin-Tate extension which is the splitting field of  $e(X)$  over  $K_p$  and contains  $\sqrt[3]{p}$ . Let  $u \in \mathbb{Z}_p^\times(1+p\mathcal{O}_p)$ . Since  $[u]_{\mathcal{F}}(e(X)) = e([u]_{\mathcal{F}}(X))$ ,  $[u]_{\mathcal{F}}(\omega_p^{p^2-1}\sqrt[3]{p}) = \omega_p^l \omega_p^{p^2-1}\sqrt[3]{p}$  for some integer  $l$ , where  $\omega_{p^2-1}$  is a primitive  $(p^2-1)$ -th root of unity. If  $u \equiv \omega_{p^2-1}^{(p+1)m} \pmod{p}$  for some integer  $m$ ,  $[u]_{\mathcal{F}}(\omega_p^{p^2-1}\sqrt[3]{p}) \equiv \omega_{p^2-1}^{(p+1)m} \omega_p^{p^2-1}\sqrt[3]{p} \pmod{(\omega_p^{p^2-1}\sqrt[3]{p})^2}$ . Since  $\omega_{p^2-1}^l - \omega_{p^2-1}^{(p+1)m}$  is either zero or a  $p$ -adic unit, we conclude that  $\omega_{p^2-1}^l = \omega_{p^2-1}^{(p+1)m}$  and  $[u]_{\mathcal{F}}(\omega_p^{p^2-1}\sqrt[3]{p}) = \omega_{p^2-1}^{(p+1)m} \omega_p^{p^2-1}\sqrt[3]{p}$ . Hence

$$[u]_{\mathcal{F}}(\sqrt[3]{p}) = (\omega_{p^2-1}^{(p+1)m} \omega_p^{p^2-1}\sqrt[3]{p})^{\frac{p^2-1}{3}} = \sqrt[3]{p}.$$

Thus  $\mathbb{Z}_p^\times(1+p\mathcal{O}_p)$  fixes  $L$ .

Next we show that  $N_{L_3/K_3}(\mathcal{O}_{L,3}^\times) = \mathbb{Z}_3^\times(1+3\mathcal{O}_3)$ . Let  $L_3$  be the local field of  $L$  at the unique prime ideal above 3 and  $\mathcal{O}_{L,3}$  is the ring of integers of  $L_3$ . Note in  $L_3$ ,  $(1+\sqrt[3]{p})(1+\omega\sqrt[3]{p})(1+\omega^2\sqrt[3]{p}) = 1+p$ .

Since  $p \equiv 2 \pmod{3}$ , the 3-adic valuation  $\nu_3(1 + \sqrt[3]{p}) = \frac{1}{3}$ . Then  $\varpi = \frac{\sqrt{-3}}{1 + \sqrt[3]{p}}$  has 3-adic valuation  $\frac{1}{6}$ . So the 6-degree extension  $L_3/\mathbb{Q}_3$  is totally ramified and  $\varpi$  is a uniformizer. The ring of integers  $\mathcal{O}_{L,3} = \mathbb{Z}_3[\varpi]$ . Let  $x = \alpha + \beta\varpi + \gamma\varpi^2 \in \mathcal{O}_{L,3}^\times$ . Then  $\alpha \in \mathbb{Z}_3[\sqrt{-3}]^\times$  and  $\beta, \gamma \in \mathbb{Z}_3[\sqrt{-3}]$ . If  $p \equiv 2 \pmod{9}$ , then

$$\begin{aligned} N_{L_3/K_3}(x) &\equiv (\alpha + \gamma + \frac{\sqrt{-3}}{3}\beta)^3 + (-\frac{\sqrt{-3}}{3}\beta)^3 p + (-\gamma + \frac{\sqrt{-3}}{3}\beta)^3 p^2 \\ &\quad - 3p(-\frac{\sqrt{-3}}{3})\beta(\alpha + \gamma + \frac{\sqrt{-3}}{3}\beta)(-\gamma + \frac{\sqrt{-3}}{3}\beta) \\ &\equiv \sqrt{-3}\beta(\alpha^2 - \beta^2) + A \pmod{3\mathcal{O}_3}, \end{aligned}$$

where  $A \in \mathbb{Z}_3$ . If  $p \equiv 5 \pmod{9}$ , then

$$\begin{aligned} N_{L_3/K_3}(x) &\equiv (\alpha - \frac{\sqrt{-3}}{3}\beta)^3 + (\frac{\sqrt{-3}}{3}\beta - \gamma)^3 p + (-\frac{\sqrt{-3}}{3}\beta - \gamma)^3 p^2 \\ &\quad + 3p(\alpha - \frac{\sqrt{-3}}{3}\beta)(\frac{\sqrt{-3}}{3}\beta - \gamma)(-\frac{\sqrt{-3}}{3}\beta - \gamma) \\ &\equiv \sqrt{-3}\beta(\beta^2 - \alpha^2) + B \pmod{3\mathcal{O}_3}, \end{aligned}$$

where  $B \in \mathbb{Z}_3$ . Since  $\alpha \in \mathbb{Z}_3[\sqrt{-3}]^\times$ ,  $\beta(\alpha^2 - \beta^2) \in \sqrt{-3}\mathcal{O}_3$ . Hence  $N_{L_3/K_3}(\mathcal{O}_{L,3}^\times) \subset \mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)$ . By local class field theory,  $\text{Gal}(L_3/K_3) \simeq \mathcal{O}_3^\times/N_{L_3/K_3}(\mathcal{O}_{L,3}^\times)$ , because  $(\sqrt{-3})$  is totally ramified in  $L_3/K_3$ . Since  $\mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)$  has index 3 in  $\mathcal{O}_3^\times$ , we see that  $N_{L_3/K_3}(\mathcal{O}_{L,3}^\times) = \mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)$ .

Since  $L/K$  is unramified outside  $(\sqrt{-3})$  and  $(p)$ ,  $K^\times \mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)\mathcal{O}_p^{\times 3}(1 + p\mathcal{O}_p)\hat{\mathcal{O}}_K^{\times(3p)}$  is contained in  $K^\times N_{L/K}(\hat{L}^\times)$ . Since it has index 3 in  $\hat{K}^\times$ ,  $K^\times N_{L/K}(\hat{L}^\times) = K^\times \mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)\mathcal{O}_p^{\times 3}(1 + p\mathcal{O}_p)\hat{\mathcal{O}}_K^{\times(3p)}$  and the Galois group  $\text{Gal}(L/K)$  is isomorphic to  $\mathcal{O}_3^\times/\mathbb{Z}_3^\times(1 + 3\mathcal{O}_3) = \langle \sigma_{\omega_3} \rangle$  and is also isomorphic to  $\mathcal{O}_p^\times/\mathcal{O}_p^{\times 3}(1 + p\mathcal{O}_p) = \langle \sigma_{\omega_p} \rangle$  with  $\sigma_{\omega_3}\sigma_{\omega_p} = 1$  on  $L$ . The Artin symbol  $[\omega_p, K_p^1/K_p](\sqrt[3]{p}) = [\omega_p^{-1}]_{\mathcal{F}}(\sqrt[3]{p}) = (\omega^{-1} \sqrt[3]{p}^2)^{\frac{p^2-1}{3}}$ . If  $p \equiv 2 \pmod{9}$ ,  $\sigma_{\omega_p}(\sqrt[3]{p}) = \omega^2 \sqrt[3]{p}$ . If  $p \equiv 5 \pmod{9}$ ,  $\sigma_{\omega_p}(\sqrt[3]{p}) = \omega \sqrt[3]{p}$ . Then  $\sigma_{\omega_3}(\sqrt[3]{p}^*) = \sigma_{\omega_p}^{-1}(\sqrt[3]{p}^*) = \omega(\sqrt[3]{p}^*)$ . Since  $p \equiv 2 \pmod{3}$ ,  $\mathbb{Z}_p^\times \subset \mathcal{O}_p^{\times 3}(1 + p\mathcal{O}_p)$  and then  $\hat{\mathcal{O}}_{3N}^\times$  fixes  $\sqrt[3]{p}$ . So  $\sqrt[3]{p}$  is in  $H_{3p}$ . Thus  $H_0 \subset H_{3N}$  and the norm subgroup of  $H_0$  is  $K^\times \mathbb{Z}_3^\times(1 + 3\mathcal{O}_3) \prod_{p|N} \mathcal{O}_p^{\times 3}(1 + p\mathcal{O}_p)\hat{\mathcal{O}}_K^{\times(3N)}$ , and hence, the Galois group  $\text{Gal}(H_0/K) = \langle \sigma_{\omega_p} | p | N \rangle$ .

The field extension  $K(\sqrt[3]{2})$  is totally ramified at 2 and 3 and unramified elsewhere. It can be showed in a completely same manner with the prime  $p$  replaced by 2 that  $\hat{\mathcal{O}}_6^\times = (1 + 2\mathcal{O}_2)\mathbb{Z}_3^\times(1 + 3\mathcal{O}_3)\hat{\mathcal{O}}_K^{\times(6)}$  fixes  $\sqrt[3]{2}$ . Since  $K^\times \hat{\mathcal{O}}_6^\times$  has index 3 in  $\hat{K}^\times$ ,  $K(\sqrt[3]{2})$  is the class field  $H_6$  and  $\text{Gal}(H_6/K) \simeq \mathcal{O}_2^\times/(1 + 2\mathcal{O}_2) = \langle \sigma_{\omega_2} \rangle$  and  $\sigma_{\omega_2}(\sqrt[3]{2}) = \omega^2 \sqrt[3]{2}$ . Since the field extension  $H_{3N}/K$  is unramified at the prime ideal  $(2)$ ,  $\sqrt[3]{2}$  cannot be contained in  $H_{3N}$  and, hence  $H_{6N} = H_{3N}(\sqrt[3]{2})$  and  $\text{Gal}(H_{6N}/H_{3N}) \simeq \mathcal{O}_2^\times/(1 + 2\mathcal{O}_2) = \langle \sigma_{\omega_2} \rangle$ .  $\square$

Let  $T = (-\sqrt[3]{4}, \sqrt{-3})$  be a point in  $E[3](H_6)$ . By Proposition 2.7,

$$T^{\sigma_{\omega_2}} = T^{\sigma_{\omega_3}^{-1}} = [\omega]T = T + \tau(2).$$

Then  $P_0 - T$  is a point in  $E(H_{3N})$  by Proposition 2.7 and Corollary 2.6. Let  $y_0 = \text{Tr}_{H_{3N}/H_0}(P_0 - T) \in E(H_0)$ .

**Proposition 2.8.** a. *The point  $y_0 \in E(H_0)$  satisfies*

$$y_0^{\sigma_{\omega_3}} = [\omega]y_0 + t,$$

where  $t \in E(\mathbb{Q})[3]$  is a nonzero point, and

$$\overline{y_0} = [-1]y_0.$$

b. *The point  $y_0 \in E(H_0)$  is of infinite order. In particular, the point*

$$z_0 = \text{Tr}_{H_{6N}/H_0}P_0 = 3y_0$$

*is of infinite order in  $E(H_0)$ .*

*Proof.* We have

$$\begin{aligned}
y_0^{\sigma_{\omega_3}} &= \text{Tr}_{H_{3N}/H_0}(P_0^{\sigma_{\omega_3}} - T^{\sigma_{\omega_3}}) \\
&= \text{Tr}_{H_{3N}/H_0}([\omega]P_0) - [\omega]^2 T \\
&= \text{Tr}_{H_{3N}/H_0}([\omega](P_0 - T) + [\omega - \omega^2]T) \\
&= \text{Tr}_{H_{3N}/H_0}([\omega](P_0 - T) + \tau(4)) \\
&= [\omega]y_0 + t,
\end{aligned}$$

where  $t = \prod_{p|N} \frac{p+1}{3} \tau(4)$  is a torsion point of order 3, because  $\prod_{p|N} \frac{p+1}{3}$  is prime to 3. Clearly, one has  $\overline{y_0} = [-1]y_0$ . The first assertions follows.

Next we prove the second assertion. We show that  $E(H_0)[3^\infty] = E(K)[3^\infty]$ . Assume  $E(H_0)[3^\infty] \neq E(K)[3^\infty]$  and let  $P$  be a point in  $E(H_0)[3^\infty] \setminus E(K)$ . Then  $K(P)/K$  is unramified outside 2, 3. Meanwhile,  $K(P)$  must contains some  $\sqrt[3]{d}$ , with some  $d = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k} \neq 1$ . Then  $K(P)/K$  is ramified at the primes  $p_i$  with  $\epsilon_i \neq 0$ . This is a contradiction. So  $E(H_0)[3^\infty] = E(K)[3^\infty]$ .

Let  $C$  be a sufficiently large integer prime to 3 that kills points in  $E(H_0)_{\text{tor}}$  of order prime to 3. If  $y_0$  is torsion, then  $Cy_0 \in E(H_0)[3^\infty] = E(K)[3^\infty]$  satisfies

$$Cy_0 = Cy_0^{\sigma_{\omega_3}} = [\omega]Cy_0 + Ct,$$

where  $Ct \in E(\mathbb{Q})[3]$  is nonzero by the first assertion. Then the torsion point  $t$  is divisible by  $[1 - \omega]$  which implies that it is killed by  $[2]$  because  $E(K) = E[2\sqrt{-3}]$  and this conflicts with the fact the point  $t$  has order 3. Hence,  $y_0$  is a point of infinite order in  $E(H_0)$  as required.

Finally,  $z_0 = \text{Tr}_{H_{6N}/H_0}(P_0 - T + T) = 3y_0 + \text{Tr}_{H_{6N}/H_0}T$ . Since  $\text{Gal}(H_{6N}/H_{3N}) = \langle \sigma_{\omega_2} \rangle$ ,

$$\text{Tr}_{H_{6N}/H_{3N}}T = T + T^{\sigma_{\omega_2}} + T^{\sigma_{\omega_2}^2} = [1 + \omega + \omega^2]T = 0.$$

Hence,  $z_0 = 3y_0$  is of infinite order. □

*Proof of Theorem 1.1.* We note that

$$\sum_d z_d = 3^k z_0,$$

where  $d$  runs through all  $d = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k}$  with  $\epsilon_i = -1, 0, 1$ . We will examine for which  $d$  the terms  $z_d$  will contribute on the left hand side.

If  $k = 1$ , using Proposition 2.7 and Proposition 2.8, one can easily compute that  $z_1 = z_{p_1^{*-1}} = 0$  and  $z_{p_1^*} = 3z_0$ .

Assume  $k \geq 2$ . Let  $d = p_1^{*\epsilon_1} p_2^{*\epsilon_2} \cdots p_k^{*\epsilon_k}$ , where  $\epsilon_i = -1, 0, 1$ . Since  $p_i \equiv 2 \pmod{3}$ ,  $1 \leq i \leq k$ , they are inert in  $K$  and hence  $E$  is supersingular at these primes. So the Fourier coefficients  $a_{p_i} = 0$  for the new form of level  $\Gamma_0(36)$  and, by the Euler system property of CM points, see [19], if  $\epsilon_i = 0$  for some  $i$ , then  $\text{Tr}_{H_{6N}/H_{6N/p_i}}P_0 = 0$  and consequently  $z_d = 0$ .

Since  $y_0^{\sigma_{\omega_3}} = [\omega]y_0 + t$ , for some nonzero  $t \in E(\mathbb{Q})[3]$ , we have

$$\left( \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 \right)^{\sigma_{\omega_3}} = [\omega] \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 \in E(K(\sqrt[3]{d})).$$

By Proposition 2.7,

$$\chi_d(\sigma_{\omega_3}) = (\sqrt[3]{d})^{\sigma_{\omega_3}-1} = \omega^{\sum_{i=1}^k \epsilon_i}.$$

If  $3 \mid \sum_{i=1}^k \epsilon_i$ , in which case the epsilon factor  $\epsilon(E, \chi_d) = +1$ , then  $(\sqrt[3]{d})^{\sigma_{\omega_3}-1} = 1$  and  $\sigma_{\omega_3} = 1$  on  $K(\sqrt[3]{d})$ . Then

$$\text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 = \left( \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 \right)^{\sigma_{\omega_3}} = [\omega] \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0.$$

So  $[1 - \omega] \left( \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 \right) = 0$  and therefore  $\text{Tr}_{H_0/K}(\sqrt[3]{d})z_0 = 3 \text{Tr}_{H_0/K}(\sqrt[3]{d})y_0 = 0$ . Then we have

$$z_d = \sum_{\sigma \in \text{Gal}(K(\sqrt[3]{d})/K)} [\chi_d^{-1}(\sigma)] \left( \text{Tr}_{H_0/K}(\sqrt[3]{d})z_0 \right)^\sigma = 0.$$

If  $3 \nmid \sum_{i=1}^k \epsilon_i$ , in which case the epsilon factor  $\epsilon(E, \chi_d) = -1$ , then  $(\sqrt[3]{d})^{\sigma_{\omega_3}-1} \neq 1$  and  $\text{Gal}(K(\sqrt[3]{d})/K) = \langle \sigma_{\omega_3} \rangle$ . We have

$$\left( \text{Tr}_{H_0/K}(\sqrt[3]{d})z_0 \right)^{\sigma_{\omega_3}} = [\omega] \text{Tr}_{H_0/K}(\sqrt[3]{d})z_0.$$

and then

$$z_d = \begin{cases} 3\mathrm{Tr}_{H_0/K(\sqrt[3]{d})} z_0, & \sum_{i=1}^k \epsilon_i \equiv 1 \pmod{3}; \\ 0, & \sum_{i=1}^k \epsilon_i \equiv 2 \pmod{3}. \end{cases}$$

Thus we have an identity

$$3^k z_0 = \sum_{\substack{d=p_1^{*\epsilon_1} p_2^{*\epsilon_2} \cdots p_k^{*\epsilon_k} \\ \forall i \ \epsilon_i \neq 0 \\ \sum_{i=1}^k \epsilon_i \equiv 1 \pmod{3}}} z_d$$

in  $E(H_0)$ . Here the condition  $\sum_{i=1}^k \epsilon_i \equiv 1 \pmod{3}$  exactly means that  $\epsilon(1, E, \chi_d) = -1$  and  $\epsilon(E^{(d)}) = -1$ . Since  $z_0$  is of infinite order, at least one of such  $z_d \in E(K(\sqrt[3]{d}))^{\chi_d}$  is of infinite order, and this produces a nonzero point in  $E^{(d)}(K)_{\mathbb{Q}}$ . Then by the Gross-Zagier formula,  $L(1, E^{(d^{-1})}) \neq 0$  and hence  $E^{(d^{-1})}(\mathbb{Q})$  is torsion and  $2d^{-1}$  is not a cube sum.

Thus for arbitrary integer  $k \geq 1$ , and arbitrary primes  $p_1, p_2, \dots, p_k$  which are all congruent to  $2, 5 \pmod{9}$ , there exists a cube-free integer  $n$  with exactly prime factors  $p_1, p_2, \dots, p_k$  such that  $2n$  is a cube sum (resp. not a cube sum). The theorem follows.  $\square$

### 3. AN EXPLICIT GROSS-ZAGIER FORMULA

In this section, we generalize the construction of the Heegner point  $z_n$  in the cube sum problem to a very general framework. A height formula for this Heegner point is then obtained as an application of the variation of Gross-Zagier formula in [3] Theorem 1.6.

**Local Theory.** Let  $F$  be a nonarchimedean local field of characteristic zero. For  $F$ , denote by  $\mathcal{O}$  the ring of integers in  $F$ ,  $\omega$  a uniformizer,  $\mathfrak{p}$  its maximal ideal and  $q$  the cardinality of its residue field. Let  $B$  be a quaternion algebra defined over  $F$  with a quadratic  $F$ -subalgebra  $K$ . Let  $e$  be the ramification index of  $K/F$  if  $K$  is nonsplit. Denote by  $G$  the algebraic group  $B^\times$  over  $F$  and also write  $G$  for  $G(F)$ . Let  $\pi$  be an irreducible admissible representation of  $G$  which is always assumed to be generic if  $G \cong \mathrm{GL}_2$ . Denote by  $\omega$  the central character of  $\pi$ . Let  $\chi$  be a character on  $K^\times$  such that  $\chi|_{F^\times} \cdot \omega = 1$ . Let  $\mathcal{P}(\pi, \chi)$  be the functional space  $\mathrm{Hom}_{K^\times}(\pi, \chi^{-1})$ . By a theorem of Tunnell and Saito, the space  $\mathcal{P}(\pi, \chi)$  has dimension at most one and equals one if and only if

$$\epsilon(\pi, \chi) = \chi\eta(-1)\epsilon(B).$$

Here,  $\epsilon(\pi, \chi)$  is the Rankin-Selberg root number for  $\sigma \times \pi_\chi$  where  $\sigma$  is the Jacquet-Langlands lifting of  $\pi$  to  $\mathrm{GL}_2(F)$  and  $\pi_\chi$  is the representation on  $\mathrm{GL}_2(F)$  constructed from  $\chi$  via Weil representation. The quadratic character  $\eta$  corresponds to the extension  $K/F$  via class field theory and  $\epsilon(B) = +1$  (resp.  $-1$ ) if  $B$  is split (resp. division).

For our purpose, assume (1) the central character  $\omega$  is unramified (2) the pair  $(\pi, \chi)$  is essentially unitary in the sense that there exists some character  $\mu = |\cdot|^s$  on  $F^\times$  with  $s \in \mathbb{C}$  such that both  $\pi \otimes \mu$  and  $\chi \otimes \mu_K^{-1}$  are unitary. Here for a character  $\mu$ ,  $\mu_K$  is the composition of  $\mu$  with the norm map from  $K$  to  $F$ . Modify  $(\pi, \chi)$  to  $(\pi \otimes \mu, \chi \otimes \mu_K^{-1})$  for some  $\mu$ , we may from now on assume that  $\pi$  and  $\chi$  are both unitary while  $\pi$  has trivial central character.

Denote by  $n$  the conductor of  $\sigma$ , that is, the minimal non-negative integer  $n$  such that the invariant subspace of  $\sigma^{U_0(n)}$  is nonzero where

$$U_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}) \mid c \in \mathfrak{p}^n \right\}.$$

Let  $c$  be the minimal non-negative integer such that  $\chi$  is trivial on  $\mathcal{O}_c^\times$  where  $\mathcal{O}_c = \mathcal{O} + \varpi^c \mathcal{O}_K$  and  $\mathcal{O}_K$  is the ring of integers for  $K$ .

**Lemma 3.1.** *Let the pair  $(\pi, \chi)$  be as above such that  $\epsilon(\pi, \chi) = \chi\eta(-1)\epsilon(B)$ . If  $K$  is nonsplit and  $c - n + e - 1 \geq 0$ , then  $B$  is split.*

*Proof.* If  $c \geq n$  or  $n \geq 3$ , then  $B$  is split (see [3] Lemma 3.1 (5) and its proof). In the following, assume  $K/F$  is ramified,  $n = 2$  and  $c = 1$ . Assume  $\pi$  is on  $\mathrm{GL}_2(F)$  and square-integrable. If  $\pi = \mathrm{sp}(2) \otimes \mu$ , then  $\mu$  is a quadratic character on  $F^\times$  with conductor 1. By [3], Lemma 3.1 (3),  $B$  is nonsplit if and only if  $\mu_K \cdot \chi = 1$ . Since  $\mu_K|_{F^\times} = 1$  and the conductor of  $\mu$  is 1,  $\mu_K$  is unramified. Hence, in this case,

$B$  must be split. If  $\pi$  is supercuspidal, then by [31], Lemma 3.2, the two unramified characters in the dual of  $K^\times/F^\times$  appear in  $\pi_0$ . Here,  $\pi_0$  is the irreducible representation on the division algebra whose Jacquet-Langlands lifting is  $\pi$ . Since  $\pi_0$  has dimension two, all the ramified characters should occur in  $\pi$  and  $B$  is split.  $\square$

Let  $(\cdot, \cdot)$  be any non-degenerate invariant Hermitian pairing on  $\pi$ . For any  $f \in \pi$ , denote by

$$\beta^0(f) = \int_{F^\times \backslash K^\times} \frac{(\pi(t)f, f)}{(f, f)} \chi(t) dt$$

where  $dt$  is any Haar measure on  $F^\times \backslash K^\times$ . The integral is absolutely convergence. The functional space  $\mathcal{P}(\pi, \chi)$  is nontrivial if and only if  $\beta^0$  is nontrivial. If  $\mathcal{P}(\pi, \chi)$  is nonzero, a nonzero vector  $f$  of  $\pi$  is called a *test vector* for  $\mathcal{P}(\pi, \chi)$  if  $\ell(f) \neq 0$  for some (thus any) nonzero  $\ell \in \mathcal{P}(\pi, \chi)$ , or equivalently,  $\beta^0(f)$  is non-vanishing.

We shall end our discussion of local theory by the following lemma which will be used in the proof of main result Theorem 3.5

**Lemma 3.2.** *Assume  $K/F$  is ramified,  $cn \neq 0$  with  $c+1 = n$ . Let  $B$  be split. Let  $R$  be an order in  $B$  with discriminant  $n$  such that  $R = R' \cap R''$ . Here  $R'$  and  $R''$  are two maximal orders in  $B$  such that  $R' \cap K = \mathcal{O}_c$  and  $R'' \cap K = \mathcal{O}_K$ . Such order exists and unique up to  $K^\times$ -conjugacy. The invariant subspace  $\pi^{R^\times}$  is of dimension 1. For any nonzero  $f \in \pi^{R^\times}$ ,*

$$\beta^0(f) = 2^{-1} q^{-c} \text{Vol}(K^\times/F^\times) L(1, 1_F).$$

*Proof.* The existence and uniqueness of the order  $R$  follows from [3] Lemma 3.2. The order  $R$  is an Eichler order. In particular, if we fix an isomorphism  $B \cong M_2(F)$ , then  $R^\times$  is  $\text{GL}_2(F)$ -conjugate to  $U_0(n)$ . By new form theory, the invariant subspace  $\pi^{R^\times}$  is of dimension one. Next, we compute the local toric integral  $\beta^0(f)$  for any  $f$ . It is similar to that in [3] §3.4. Let  $\tau$  be a uniformizer of  $K$  such that  $\mathcal{O}_K = \mathcal{O}[\tau]$  and embed  $K$  into  $M_2(F)$  by

$$a + b\tau \mapsto \gamma_c^{-1} \begin{pmatrix} a + b\text{tr}\tau & bN\tau \\ -b & a \end{pmatrix} \gamma_c, \quad \gamma_c = \begin{pmatrix} \varpi^c N\tau & \\ & 1 \end{pmatrix},$$

where  $\omega$  is a uniformizer of  $F$  and  $\text{ord}_v(c_v)$  is denoted by  $c$ . In particular, under this embedding,  $R_0(n) = \begin{pmatrix} \mathcal{O} & \mathcal{O} \\ \mathfrak{p}^n & \mathcal{O} \end{pmatrix}$  is an admissible order for  $(\pi, \chi)$ . Since the toric integral is invariant under  $K^\times$ -conjugacy of  $f$ , we may take  $R = R_0(n)$  and  $f = f_0$  the normalized new form of  $\pi$ . Let  $\Psi(g)$  denote the matrix coefficient

$$\Psi(g) := \frac{(\pi(g)f_0, f_0)}{(f_0, f_0)}, \quad g \in \text{GL}_2(F).$$

Then  $\Psi$  is a function on  $ZU_0(n) \backslash \text{GL}_2(F)/U_0(n)$  where  $Z$  is the center of  $\text{GL}_2(F)$  and

$$\beta(f) = \frac{\text{Vol}(K^\times/F^\times)}{\#K^\times/F^\times \mathcal{O}_c^\times} \sum_{t \in K^\times/F^\times \mathcal{O}_c^\times} \Psi(t) \chi(t).$$

Denote by

$$S_i = \{1 + b\tau, b \in \mathcal{O}/\mathfrak{p}^c, v(b) = i\}, \quad 0 \leq i \leq c-1$$

and

$$S' = \{a\varpi + \tau, a \in \mathcal{O}/\mathfrak{p}^c\}.$$

Then a complete representatives of  $K^\times/F^\times \mathcal{O}_c^\times$  can be taken as

$$\{1\} \sqcup (\sqcup_i S_i) \sqcup S'.$$

Let  $\text{pr} : K^\times \rightarrow ZU_0(n) \backslash \text{GL}_2(F)/U_0(n)$  be the natural mapping. Then it is constant on  $S_i$  and  $S'$ . Precisely,

$$\text{pr}(S_i) = \left[ \begin{pmatrix} 1 & \varpi^{i-c} \\ & 1 \end{pmatrix} \right], \quad \text{pr}(S') = \left[ \begin{pmatrix} & \varpi^{-c} \\ -\varpi^{c+1} & \end{pmatrix} \right].$$

Follow from this

$$\sum_{t \in K^\times/F^\times \mathcal{O}_c^\times} \Psi(t) \chi(t) = 1 + \sum_{i=0}^{c-1} \Psi_i \sum_{t \in S_i} \chi(t) + \Psi' \sum_{t \in S'} \chi(t),$$

where  $\Psi_i$  (resp.  $\Psi'$ ) are the valuations of  $\Psi(t)$  on  $S_i$  (resp.  $S'$ ). As

$$\sum_{t \in S_i} \chi(t) = \begin{cases} 0, & \text{if } c > 1 \text{ and } 0 \leq i \leq c-2, \\ -1, & \text{if } i = c-1, \end{cases} \quad \text{and} \quad \sum_{t \in S'} \chi(t) = 0,$$

we obtain,

$$\sum_{t \in K^\times / F^\times \mathcal{O}_c^\times} \Psi(t) \chi(t) = 1 - \Psi_{c-1}.$$

Finally, one needs to compute this matrix coefficient. However, as it actually evaluates at some upper-triangular matrix, the computation is easy by the explicit description of normalized new forms in Kirillov model. In fact,  $\Psi_{c-1} = -q^{-1}L(1, 1_F)$  where  $q$  is the cardinality of the residue field of  $F$  (See also [3] §3.4). Thus

$$\beta^0(f) = \frac{\text{Vol}(K^\times / F^\times)}{\#K^\times / F^\times \mathcal{O}_c^\times} L(1, 1_F) = 2^{-1} q^{-c} \text{Vol}(K^\times / F^\times) L(1, 1_F).$$

□

**Global Theory.** Let  $F$  be a totally real field with  $\mathcal{O}$  its ring of integers. Take  $d := [F : \mathbb{Q}]$ . Denote by  $\mathbb{A} = F_{\mathbb{A}}$  be the adele ring of  $F$  and  $\mathbb{A}_f$  its finite part. For a  $\mathbb{Z}$ -module  $M$ , take  $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$  with  $\widehat{\mathbb{Z}} = \prod_{p < \infty} \mathbb{Z}_p$ . Let  $\mathbb{B}$  be a totally definite incoherent quaternion algebra over  $\mathbb{A}$ . For any open compact subgroup  $U$  of  $\mathbb{B}_f^\times = (\mathbb{B} \otimes_{\mathbb{A}} \mathbb{A}_f)^\times$ , denote by  $X_U$  the Shimura curve associated to  $\mathbb{B}^\times$  of level  $U$ . Denote by  $\xi_U \in \text{Pic}(X_U)_{\mathbb{Q}}$  the normalized Hodge class on  $X_U$ . Let  $X$  be the projective limit of the system  $(X_U)_U$ . Let  $A$  be a simple abelian variety defined over  $F$  parametrized by  $X$  in the sense that there is a non-constant morphism  $X_U \rightarrow A$  over  $F$  for some  $U$ . Then  $M := \text{End}^0(A)$  is a field. Denote by  $\pi = \pi_A = \varinjlim_U \text{Hom}_{\xi_U}^0(X_U, A)$ . Here,  $\text{Hom}_{\xi_U}^0(X_U, A)$  denotes the morphisms in  $\text{Hom}(X_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$  using  $\xi_U$  as a base point: if  $\xi_U$  is represented by a divisor  $\sum_i a_i x_i$  on  $X_{U, \bar{F}}$ , then  $f \in \text{Hom}_F(X_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$  is in  $\pi_A$  if and only if  $\sum a_i f_i(x_i) = 0$  in  $A(\bar{F})_{\mathbb{Q}} = A(\bar{F}) \otimes_{\mathbb{Z}} \mathbb{Q}$ . For each open compact subgroup  $U$  of  $\mathbb{B}_f^\times$ , let  $J_U$  denote the Jacobian of  $X_U$ . Then  $\pi = \varinjlim_U \text{Hom}^0(J_U, A)$  where  $\text{Hom}^0(J_U, A) = \text{Hom}_F(J_U, A) \otimes_{\mathbb{Z}} \mathbb{Q}$ . The Hecke action of  $\mathbb{B}^\times$  on  $X$  induces a natural  $\mathbb{B}^\times$ -module structure on  $\pi$  so that  $\text{End}_{\mathbb{B}^\times}(\pi) = M$  and has a decomposition  $\pi = \otimes_M \pi_v$  where  $\pi_v$  are absolutely irreducible representations of  $\mathbb{B}_v^\times$  over  $M$ . Let  $N$  be the conductor of the Jacquet-Langlands lifting of  $\pi$ . Denote by  $\omega_A$  its central character. Let  $A^\vee$  be the dual abelian variety of  $A$ . There is a perfect  $\mathbb{B}^\times$ -invariant pairing

$$\pi_A \otimes \pi_{A^\vee} \longrightarrow M$$

given by

$$(f_1, f_2) = \text{Vol}(X_U)^{-1} (f_{1,U} \circ f_{2,U}^\vee), \quad f_{1,U} \in \text{Hom}(J_U, A), f_{2,U} \in \text{Hom}(J_U, A^\vee)$$

where  $f_{2,U}^\vee : A \rightarrow J_U$  is the dual of  $f_{2,U}$  composed with the canonical isomorphism  $J_U^\vee \cong J_U$ . Here,  $\text{Vol}(X_U)$  is defined by a fixed invariant measure on the upper half plane. It follows that  $\pi_{A^\vee}$  is dual to  $\pi_A$  as representations of  $\mathbb{B}^\times$  over  $M$ . For any fixed open compact subgroup  $U$  of  $\mathbb{B}_f^\times$ , define the  $U$ -pairing on  $\pi_A \times \pi_{A^\vee}$  by

$$(f_1, f_2)_U = \text{Vol}(X_U) (f_1, f_2), \quad f_1 \in \pi_A, f_2 \in \pi_{A^\vee}$$

which is independent of the choice of measure defining  $\text{Vol}(X_U)$ .

Let  $K$  be a totally imaginary quadratic extension over  $F$  with relative discriminant  $D = D_{K/F} \subset \mathcal{O}$  and absolute discriminant  $D_K$ . Denote by  $\mathcal{O}_K$  its ring of integers. Let  $\eta$  be the quadratic character corresponding to  $K/F$ . Take  $\chi : K^\times \backslash K_{\mathbb{A}}^\times \rightarrow L^\times$  a character of finite order where  $L$  is a finite extension on  $M$ . Let  $c \subset \mathcal{O}$  be the ideal maximal such that  $\chi$  is trivial on  $\prod_{v \nmid c} \mathcal{O}_{K,v}^\times \prod_{v \mid c} (1 + c\mathcal{O}_{K,v})$ . Assume that  $\omega_A \cdot \chi|_{\mathbb{A}_f^\times} = 1$  and for any place  $v$ ,

$$\epsilon(\pi_v, \chi_v) = \chi_v \eta_v(-1) \epsilon(\mathbb{B}_v),$$

where  $\epsilon(\mathbb{B}_v) = 1$  if  $\mathbb{B}_v$  is split or  $-1$  otherwise and  $\epsilon(\pi_v, \chi_v)$  is the local root number of the Rankin-Selberg  $L$ -series  $L(s, \pi, \chi)$ . These assumptions imply that the Rankin-Selberg root number  $\epsilon(\pi, \chi) = -1$  and there exists an embedding  $K_{\mathbb{A}}^\times \rightarrow \mathbb{B}^\times$ . Let  $X^{K^\times}$  be the  $F$ -subscheme of  $X$  of fixed points of  $X$  under  $K^\times$ . The theory of complex multiplication asserts that every point in  $X^{K^\times}(\bar{F})$  is defined over  $K^{\text{ab}}$  and



that the Galois action is given by the Hecke action under the reciprocity law. Let  $P \in X^{K^\times}(K^{\text{ab}})$ . For any  $f \in \pi$ , consider the Heegner cycle

$$\int_{K^\times \backslash \widehat{K}^\times / \widehat{F}^\times} f(P)^{\sigma_t} \chi(t) dt \in A(K^{\text{ab}})_{\mathbb{Q}} \otimes_M L$$

where  $\sigma : K^\times \backslash \widehat{K}^\times / \widehat{F}^\times \rightarrow \text{Gal}(K^{\text{ab}}/K)$  is the Artin map. The main result in the book of Yuan-Zhang-Zhang [33] implies that there is some  $f \in \pi$  such that the corresponding Heegner cycle for  $f$  is nonvanishing if and only if  $L'(1, A, \chi)$  is nonvanishing.

In the following, we shall explicit construct a one-dimensional  $L$ -subspace  $V(\pi, \chi)$  of  $\pi \otimes_M L$  such that for any nonzero  $f \in V(\pi, \chi)$ , the Heegner cycle for  $f$  is nonzero if and only if  $L'(1, A, \chi)$  is nonzero. A similar one-dimensional  $L$ -subspace is considered in [3] which is also denoted by  $V(\pi, \chi)$  there. Any vectors in these two  $L$ -lines are of pure tensor form. In fact, any two vectors from these two  $L$ -lines respectively are parallel at any places outside

$$\mathbb{S} := \left\{ v \mid (c, N) \Big| K_v/F_v \text{ is ramified and } \text{ord}_v(c) + 1 = \text{ord}_v(N) \right\}.$$

From now on, we require that the central character  $\omega$  is unramified at any place in  $\mathbb{S}$ . Define the following sets of places  $v$  of  $F$  dividing  $N$ :

$$\Sigma_1 := \{ v \mid N \text{ nonsplit in } K : \text{ord}_v(c) = 0 \text{ or } \text{ord}_v(c) - \text{ord}_v(N) + e_v - 1 < 0 \},$$

where  $e_v$  is the ramification index of  $K$  at  $v$ . Let  $c_1 = \prod_{\mathfrak{p} \mid c, \mathfrak{p} \notin \Sigma_1} \mathfrak{p}^{\text{ord}_{\mathfrak{p}} c}$  be the  $\Sigma_1$ -off part of  $c$ ,  $N_1$  the  $\Sigma_1$ -off part of  $N$ , and  $N_2 = N/N_1$ . Denote by  $\mathcal{O}_{c_1} = \mathcal{O} + c_1 \mathcal{O}_K$ .

Let  $v$  be a place of  $F$  and  $\varpi_v$  a uniformizer of  $F_v$ . Then there exists an  $\mathcal{O}_v$ -order  $R_v$  of  $\mathbb{B}_v$  with discriminant  $N\mathcal{O}_v$  such that  $R_v \cap K_v = \mathcal{O}_{c_1, v}$ . Such order exists and unique up to  $K_v^\times$ -conjugate when  $v \nmid (c_1, N)$ . At any place  $v \mid (c_1, N)$ , by Lemma 3.1,  $\mathbb{B}_v$  is split and  $R_v$  will be taken as an Eichler order. In particular, fixing an isomorphism between  $\mathbb{B}_v$  and  $M_2(F_v)$ , then  $R_v$  is  $\text{GL}_2(F_v)$ -conjugate to the order  $\begin{pmatrix} \mathcal{O}_v & \mathcal{O}_v \\ N\mathcal{O}_v & \mathcal{O}_v \end{pmatrix}$ . However, the  $K_v^\times$ -conjugacy class of  $R_v$  needs to be determined here. Such an order  $R_v$  is called *admissible* for  $(\pi_v, \chi_v)$  if it also satisfies the following conditions (1) and (2).

- (1) If  $v \mid (c_1, N)$ , then  $R_v$  is the intersection of two maximal orders  $R'_v, R''_v$  of  $\mathbb{B}_v$  such that  $R'_v \cap K_v = \mathcal{O}_{c, v}$  and

$$R''_v \cap K_v = \begin{cases} \mathcal{O}_{c/N, v}, & \text{if } \text{ord}_v(c/N) \geq 0, \\ \mathcal{O}_{K, v}, & \text{otherwise.} \end{cases}$$

Note that for  $v \mid (c_1, N)$ , By [3] Lemma 3.2, there is a unique order, up to  $K_v^\times$ -conjugate, satisfying the condition (1) unless  $K_v$  is split and  $0 < \text{ord}_v(c_1) < \text{ord}_v(N)$ . In the case  $K_v$  is split and  $0 < \text{ord}_v(c_1) < \text{ord}_v(N)$ , there are exactly two  $K_v^\times$ -conjugacy classes of orders satisfying the condition (1), which are conjugate to each other by a normalizer of  $K_v^\times$  in  $\mathbb{B}_v^\times$ . Fix an  $F_v$ -algebra isomorphism  $K_v \cong F_v^2$  and identify  $\mathbb{B}_v$  with  $\text{End}_{F_v}(K_v)$ . Then the two classes contain respectively orders  $R_{i, v} = R'_{i, v} \cap R''_{i, v}, i = 1, 2$  as in (1) such that  $R'_{i, v} = \text{End}_{\mathcal{O}_v}(\mathcal{O}_{c, v}), i = 1, 2$ , and  $R''_{1, v} = \text{End}_{\mathcal{O}_v}((\varpi_v^{n-c}, 1)\mathcal{O}_{K_v})$  and  $R''_{2, v} = \text{End}_{\mathcal{O}_v}((1, \varpi_v^{n-c})\mathcal{O}_{K_v})$ .

- (2) If  $K_v$  is split and  $0 < \text{ord}_v(c_1) < \text{ord}_v(N)$ , then  $R_v$  is  $K_v^\times$ -conjugate to some  $R_{i, v}$  such that  $\chi_i$  has conductor  $\text{ord}_v(c)$ , where  $\chi_i, i = 1, 2$  is defined by  $\chi_1(a) = \chi_v(a, 1)$  and  $\chi_2(b) = \chi_v(1, b)$ .

**Definition 3.3.** An  $\widehat{\mathcal{O}}$ -order  $\mathcal{R}$  of  $\mathbb{B}_f$  is called *admissible* for  $(\pi, \chi)$  if for every finite place  $v$  of  $F$ ,  $\mathcal{R}_v := \mathcal{R} \otimes_{\widehat{\mathcal{O}}} \mathcal{O}_v$  is admissible for  $(\pi_v, \chi_v)$ . Note that an admissible order  $\mathcal{R}$  for  $(\pi, \chi)$  is of discriminant  $N\widehat{\mathcal{O}}$  such that  $\mathcal{R} \cap \widehat{K} = \widehat{\mathcal{O}}_{c_1}$ .

Let  $\mathcal{R}$  be an  $\widehat{\mathcal{O}}$ -order of  $\mathbb{B}_f$  which is admissible for  $(\pi, \chi)$ . Let  $U = \mathcal{R}^\times$  and  $U^{(N_2)} := \mathcal{R}^\times \cap \mathbb{B}_f^{\times(N_2)}$ . Note that for any finite place  $v \mid N_1$ ,  $\mathbb{B}_v$  must be split. Let  $Z \cong \mathbb{A}_f^\times$  denote the center of  $\mathbb{B}_f^\times$ . The group  $U^{(N_2)}$  has a decomposition  $U^{(N_2)} = U' \cdot (Z \cap U^{(N_2)})$  where  $U' = \prod_{v \nmid N_2} U'_v$  such that for any finite place  $v \nmid N_2$ ,  $U'_v = U_v$  if  $v \nmid N$  and  $U'_v \cong U_1(N)_v$  otherwise. View  $\omega$  as a character on  $Z$  and we may define a character on  $U^{(N_2)}$  by  $\omega$  on  $Z \cap U^{(N_2)}$  and trivial on  $U'$ , which we also denoted by  $\omega$ .

**Definition 3.4.** Let  $V(\pi, \chi)$  denote the space of forms  $f \in \pi_A \otimes_M L$ , which are  $\omega$ -eigen under  $U^{(N_2)}$ , and  $\chi_v^{-1}$ -eigen under  $K_v^\times$  for all places  $v \in \Sigma_1$ . The space  $V(\pi, \chi)$  is actually a one dimensional  $L$ -space.

For any  $f \in V(\pi, \chi)$ , define the Heegner cycle associated to  $(\pi, \chi)$  to be

$$P_\chi(f) := \sum_{t \in \widehat{K}^\times / K^\times \widehat{F}^\times \widehat{\mathcal{O}}_{c_1}^\times} f(P)^{\sigma_t} \chi(t) \in A(K^{\text{ab}})_{\mathbb{Q}} \otimes_M L.$$

The Neron-Tate height pairing over  $K$  gives a  $\mathbb{Q}$ -linear map  $\langle \cdot, \cdot \rangle_K : A(\bar{K})_{\mathbb{Q}} \otimes_M A^\vee(\bar{K})_{\mathbb{Q}} \rightarrow \mathbb{R}$ . Let  $\langle \cdot, \cdot \rangle_{K,M} : A(\bar{K})_{\mathbb{Q}} \otimes_M A^\vee(\bar{K})_{\mathbb{Q}} \rightarrow M \otimes_{\mathbb{Q}} \mathbb{R}$  be the unique  $M$ -bilinear pairing such that  $\langle \cdot, \cdot \rangle_K = \text{tr}_{M \otimes_{\mathbb{R}} / \mathbb{R}} \langle \cdot, \cdot \rangle_{K,M}$ . This induces a  $L$ -linear Neron-Tate pairing over  $K$ :

$$\langle \cdot, \cdot \rangle_{K,L} : (A(\bar{K})_{\mathbb{Q}} \otimes_M L) \otimes (A^\vee(\bar{K})_{\mathbb{Q}} \otimes_M L) \longrightarrow L \otimes_{\mathbb{Q}} \mathbb{R}.$$

Let  $\phi$  be the Hilbert new form in the Jacquet-Langlands lifting of  $\pi$  defined as following. For  $v|\infty$ , the subgroup  $\text{SO}_2(\mathbb{R})$  of  $\text{GL}_2(F_v)$  acts on  $\phi$  via the character  $k_\theta = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \mapsto e^{4\pi i \theta}$ . It is of level  $U_1(N)$  with

$$U_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\widehat{\mathcal{O}}) \left| \begin{array}{l} c \in N\widehat{\mathcal{O}} \\ d \equiv 1 \pmod{N\widehat{\mathcal{O}}} \end{array} \right. \right\}.$$

Finally,

$$L(s, \pi) = 2^d |\delta|_{\mathbb{A}}^{s-1/2} Z(s, \phi), \quad Z(s, \phi) = \int_{F^\times \backslash \mathbb{A}^\times} \phi \left[ \begin{pmatrix} a & \\ & 1 \end{pmatrix} \right] |a|_{\mathbb{A}}^{s-1/2} d^\times a$$

where the Haar measure  $d^\times a$  is chosen such that  $\text{Res}_{s=1} \int_{|a| \leq 1} |a|^{s-1} d^\times a = \text{Res}_{s=1} L(s, 1_F)$ . The Petersson norm  $(\phi, \phi)_{U_0(N)}$  is the integration of  $\phi \bar{\phi}$  with respect to the measure  $dx dy / y^2$  on the upper half plane.

**Theorem 3.5.** *Let  $F$  be a totally real field of degree  $d$ . Let  $A$  be an abelian variety over  $F$  parametrized by a Shimura curve  $X$  over  $F$  associated to an incoherent totally definite quaternion algebra  $\mathbb{B}$  over  $\mathbb{A}$ . Denote by  $\phi$  the Hilbert holomorphic newform of parallel weight 2 on  $\text{GL}_2(\mathbb{A})$  associated to  $A$ . Let  $K$  be a totally imaginary quadratic extension over  $F$  with relative discriminant  $D$  and discriminant  $D_K$ . Let  $\chi : K_{\mathbb{A}}^\times / K^\times \rightarrow L^\times$  be a finite Hecke character of conductor  $c$  over some finite extension  $L$  of  $M := \text{End}^0(A)$ . Assume that*

- (1)  $\omega_A \cdot \chi|_{\mathbb{A}^\times} = 1$ , where  $\omega_A$  is the central character of  $\pi_A$ ;
- (2) for any place  $v$  of  $F$ ,  $\epsilon(\pi_{A,v}, \chi_v) = \chi_v \eta_v(-1) \epsilon(\mathbb{B}_v)$ ;
- (3)  $\omega$  is unramified at any place in  $\mathbb{S}$ .

For any non-zero forms  $f_1 \in V(\pi_A, \chi)$  and  $f_2 \in V(\pi_{A^\vee}, \chi^{-1})$ , we have an equality in  $L \otimes_{\mathbb{Q}} \mathbb{C}$ :

$$L'(\Sigma)(1, A, \chi) = 2^{-\#(\Sigma_D)} \frac{(8\pi^2)^d (\phi, \phi)_{U_0(N)}}{(u_1)^2 \sqrt{|D_K|} \|c_1\|^2} \cdot \frac{\langle P_\chi(f_1), P_{\chi^{-1}}(f_2) \rangle_{K,L}}{(f_1, f_2)_{\mathcal{R}^\times}}.$$

In the above,

$$\Sigma = \{v | (N, Dc) | \text{if } v | N \text{ then } \text{ord}_v(c/N) \geq 0\}$$

and

$$\Sigma_D = \{v | (N, D) | v \nmid c \text{ or } 0 < \text{ord}_v(c) < \text{ord}_v(N) - 1\}.$$

The term  $c_1$  is the  $\Sigma_1$ -off part of  $c$  and  $u_1 = \# \ker(\text{Pic}(\mathcal{O}) \rightarrow \text{Pic}(\mathcal{O}_{c_1})) \cdot [\mathcal{O}_{c_1}^\times : \mathcal{O}^\times]$  while  $\|c_1\|$  is the norm of  $c_1$ .

*Proof.* The proof is an application of the variation of Gross-Zagier formula ([3] Theorem 1.6). In other words, the above height formula is derived from the explicit Gross-Zagier formula in [3] Theorem 1.5 plus some local computations. In the following proof, we shall use notations in [3] Theorem 1.5 and add the sign  $\sharp$  for any corresponding terms in Theorem 3.5. Moreover, we shall also use measures defined in [3].

By [3] Theorem 1.6, for any  $f_1^\sharp \in V^\sharp(\pi_A, \chi)$  and  $f_2^\sharp \in V^\sharp(\pi_{A^\vee}, \chi^{-1})$ ,

$$\prod_{v \in \mathbb{S}} \frac{\beta^0(f_{1,v}^\sharp, f_{2,v}^\sharp)}{\beta^0(f_{1,v}, f_{2,v})} L'(\Sigma)(1, A, \chi) = 2^{-\# \Sigma_D} \cdot \frac{(8\pi^2)^d (\phi, \phi)_{U_0(N)}}{u_1^2 \sqrt{|D_K|} \|c_1\|^2} \cdot \frac{\langle P_\chi^{c_1}(f_1^\sharp), P_{\chi^{-1}}^{c_1}(f_2^\sharp) \rangle_{K,K}}{(f_1^\sharp, f_2^\sharp)_{\mathcal{R}^\times}}.$$

The definition of  $\Sigma$  is the same as the one in Theorem 3.5. On the other hand,

$$\Sigma_D = \{v | (N, D) | \text{ord}_v(c) < \text{ord}_v(N)\} = \Sigma_D^\sharp \sqcup \mathbb{S}.$$

The term  $c_1$  is the  $\Sigma_1$ -off part of  $c$ . Note that in [3],  $\Sigma_1$  is defined as the set of places  $v|N$  nonsplit in  $K$  with  $\text{ord}_v(c) \leq \text{ord}_v(N)$ . In particular, if we denote by  $\Sigma_1^\sharp$  the corresponding set defined before Lemma 3.1, then  $\Sigma_1 = \Sigma_1^\sharp \sqcup \mathbb{S}$ . Thus,  $c_1 c_{\mathbb{S}} = c_1^\sharp$  and  $\|c_1\| = |c|_{\mathbb{S}} \|c_1^\sharp\|$ . The Heegner point

$$P_\chi^{c_1}(f_1^\sharp) = \frac{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1})}{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1^\sharp})} \sum_{t \in \text{Pic}_{K/F}(\mathcal{O}_{c_1^\sharp})} f_1^\sharp(P)^{\sigma_t} \chi(t) = \frac{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1})}{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1^\sharp})} \cdot P_\chi(f_1^\sharp)$$

and the definition of  $P_{\chi^{-1}}^{c_1}(f_2^\sharp)$  is similarly. Denote by  $\kappa_{c_1} = \ker(\text{Pic}(\mathcal{O}) \rightarrow \text{Pic}(\mathcal{O}_{c_1}))$  and similarly for  $\kappa_{c_1^\sharp}$ , then by [3] Lemma 2.3,

$$\frac{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1})}{\#\text{Pic}_{K/F}(\mathcal{O}_{c_1^\sharp})} = \frac{[\widehat{\mathcal{O}}_K^\times : \widehat{\mathcal{O}}_{c_1}^\times] [\mathcal{O}_K^\times : \mathcal{O}_{c_1}^\times]^{-1} \#\kappa_{c_1}}{[\widehat{\mathcal{O}}_K^\times : \widehat{\mathcal{O}}_{c_1^\sharp}^\times] [\mathcal{O}_K^\times : \mathcal{O}_{c_1^\sharp}^\times]^{-1} \#\kappa_{c_1^\sharp}} = \prod_{v \in \mathbb{S}} \frac{1}{[\mathcal{O}_{K,v}^\times : \mathcal{O}_{c,v}^\times]} \frac{[\mathcal{O}_{c_1}^\times : \mathcal{O}_{c_1^\sharp}^\times] \#\kappa_{c_1}}{\#\kappa_{c_1^\sharp}} = |c|_{\mathbb{S}} \frac{u_1}{u_1^\sharp}.$$

The admissible order  $\mathcal{R} = \prod_v \mathcal{R}_v$  is different with the  $\sharp$ -admissible order  $\mathcal{R} = \prod_v \mathcal{R}_v^\sharp$  exactly at  $v \in \mathbb{S}$ . For  $v \in \mathbb{S}$ ,  $\mathcal{R}_v$  is an order in  $\mathbb{B}_v$  with discriminant  $\text{ord}_v(N)$  such that  $\mathcal{R}_v \cap K_v = \mathcal{O}_{K,v}$ . By Lemma 2.2 and Lemma 3.5 in [3],

$$\frac{\text{Vol}(X_{\mathcal{R}^\times})}{\text{Vol}(X_{\mathcal{R}^\sharp \times})} = \frac{\text{Vol}(\mathcal{R}^{\sharp \times})}{\text{Vol}(\mathcal{R}^\times)} = \prod_{v \in \mathbb{S}} \frac{\text{Vol}(\mathcal{R}_v^{\sharp \times})}{\text{Vol}(\mathcal{R}_v^\times)} = L(1, 1_F)_{\mathbb{S}}^{-1}.$$

Thus

$$(f_1^\sharp, f_2^\sharp)_{\mathcal{R}^\times} = \frac{\text{Vol}(X_{\mathcal{R}^\times})}{\text{Vol}(X_{\mathcal{R}^\sharp \times})} (f_1^\sharp, f_2^\sharp)_{\mathcal{R}^\sharp \times} = L(1, 1_F)_{\mathbb{S}}^{-1} (f_1^\sharp, f_2^\sharp)_{\mathcal{R}^\sharp \times}.$$

For any place  $v \in \mathbb{S}$ , fix a  $\mathbb{B}_v^\times$ -invariant pairing  $\langle \cdot, \cdot \rangle_v$  on  $\pi_{A,v} \times \pi_{A^\vee,v}$ . For any  $f'_{1,v} \in \pi_{A,v}$  and  $f'_{2,v} \in \pi_{A^\vee,v}$  with  $\langle f'_{1,v}, f'_{2,v} \rangle_v \neq 0$ , let

$$\beta^0(f'_{1,v}, f'_{2,v}) = \int_{F_v^\times \setminus K_v^\times} \frac{\langle \pi_{A,v}(t_v) f'_{1,v}, f'_{2,v} \rangle_v}{\langle f'_{1,v}, f'_{2,v} \rangle_v} \chi_v(t_v) dt_v.$$

The test vector  $f_{1,v}$  (resp.  $f_{2,v}$ ) is the  $v$ -component of a nonzero vector in  $V(\pi_A, \chi)$  (resp.  $V(\pi_{A^\vee}, \chi^{-1})$ ). As  $v \in \mathbb{S}$ ,  $f_{1,v}$  (resp.  $f_{2,v}$ ) is  $\chi_v^{-1}$ -eigen (resp.  $\chi_v$ -eigen) under  $K_v^\times$ .

**Lemma 3.6.** *For any  $v \in \mathbb{S}$ ,*

$$\frac{\beta^0(f_{1,v}, f_{2,v})}{\beta^0(f_{1,v}^\sharp, f_{2,v}^\sharp)} = 2L(1, 1_v)^{-1} |c_v|_v^{-1}.$$

*Proof.* As this is a local computation, we shall drop the subscript ' $v$ ' in the following. The toric integral  $\beta^0$  is invariant by modifying  $(\pi, \chi)$  to  $(\pi \otimes \mu, \chi \otimes \mu_K^{-1})$  for any character  $\mu$  of  $F^\times$ . Since the central character  $\omega$  of  $\pi$  is assumed to be unramified, we may assume  $\omega = 1$ . Identify the contragredient representation  $(\pi^\vee, \chi^{-1})$  with the complex-conjugation  $(\bar{\pi}, \bar{\chi})$  and let  $(\cdot, \cdot)$  be the Hermitian pairing on  $\pi$  defined by  $(f_1, f_2) = \langle f_1, \bar{f}_2 \rangle$ . Denote by  $\beta^0(f) = \beta^0(f, \bar{f})$ . Then the ratio we need to compute becomes  $\frac{\beta^0(f)}{\beta^0(f^\sharp)}$  with  $f \in V(\pi, \chi)$  and  $f^\sharp \in V^\sharp(\pi, \chi)$ . Since  $f \in V(\pi, \chi)$  is  $\chi^{-1}$ -invariant,  $\beta^0(f) = \text{Vol}(K^\times/F^\times)$ . On the other hand, by Lemma 3.2,  $\beta^0(f^\sharp) = 2^{-1} q^{-c} \text{Vol}(K^\times/F^\times) L(1, 1_F)$ . The result is then obtained.  $\square$

Sum up,

$$L'^{(\Sigma)}(1, A, \chi) = 2^{-\#(\Sigma_D \setminus \mathbb{S})} \cdot \frac{(8\pi^2)^d (\phi, \phi)_{U_0(N)}}{(u_1^\sharp)^2 \sqrt{|D_K| \|c_1^\sharp\|^2}} \frac{\langle P_\chi(f_1^\sharp), P_{\chi^{-1}}(f_2^\sharp) \rangle_{K,K}}{(f_1^\sharp, f_2^\sharp)_{\mathcal{R}^\sharp \times}}.$$

Using notations in Theorem 3.5, this is just the formula we need to prove.  $\square$

**Proof of Theorem 1.2.** Let  $n = p_1^{*\epsilon_1} p_2^{*\epsilon_2} \cdots p_k^{*\epsilon_k}$  with  $\epsilon_i = \pm 1$  and  $\sum_1^k \epsilon_i \equiv 1 \pmod{3}$ , which is equivalent to  $\epsilon(E, \chi_n) = -1$  and  $\epsilon(E^{(n)}) = -1$ . Denote by  $N = p_1 \cdots p_k$ . Let  $f$  be the identity morphism from  $X_0(36)$  to  $E$  taking the cusp  $[\infty]$  to the identity point of  $E$ . Let  $K = \mathbb{Q}(\sqrt{-3})$  be the complex multiplication field of  $E$ . Let  $\chi_n : \text{Gal}(H_{6N}/K) \rightarrow \mathbb{C}^\times$  be the cubic character that  $\chi_n(\sigma) = \sqrt[3]{n}^{\sigma-1}$  for  $\sigma \in \text{Gal}(H_{6N}/K)$ . The Heegner point for  $\chi_n$  is defined as

$$z_n = \sum_{\sigma \in \text{Gal}(H_{6N}/K)} [\chi_n^{-1}(\sigma)] f(P_0^\sigma).$$

**Lemma 3.7.** *Let  $B$  be the incoherent quaternion algebra over  $\mathbb{Q}$  determined by the pair  $(E, \chi_n)$ . Then  $B$  is split. Let  $\pi_E$  be the cuspidal automorphic representation associated to  $E$ , then  $f \in V(\pi_E, \chi_n)$ .*

*Proof.* Note that the conductor of  $\pi_E$  is 36, the conductor  $c(\chi_n)$  of  $\chi_n$  is  $3N$ . If  $p \nmid 36$ , then  $B_p$  is split by Lemma 3.1 (1) in [3]. As 2 is inert in  $K$ ,  $B_2$  is split by Lemma 3.1 (4) in [3]. Finally,  $B_3$  is also split by Lemma 3.1. Hence  $B$  is split. We next check that  $f \in V(\pi_E, \chi_n)$ . Note that by our choice of embedding of  $K$  to  $M_2(\mathbb{Q})$ ,  $R_0(36) \cap K = \mathcal{O}_{6N}$  with  $R_0(36) = \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 36\mathbb{Z} & \mathbb{Z} \end{pmatrix}$ . It suffices to check that  $f$  is  $K_2^\times$ -invariant and  $R_0(36)_3$  is admissible for  $(\pi_{E,3}, \chi_{n,3})$ . The fact that  $f$  is  $K_2^\times$ -invariant follows from that  $K_2^\times/\mathbb{Q}_2^\times(1+2\mathcal{O}_{K,2})$  is generated by  $\omega_2$  and by Theorem 2.5, for any point  $P$  in  $X_U$ ,  $P^{\omega_2} = P + \tau(2)$ . Finally,  $R_0(36)_3 = R' \cap R''$  where  $R' = M_2(\mathbb{Z}_3)$  and  $R'' = \begin{pmatrix} \mathbb{Z}_3 & 9^{-1}\mathbb{Z}_3 \\ 9\mathbb{Z}_3 & \mathbb{Z}_3 \end{pmatrix}$ . It is then easy to check that  $R' \cap K_3 = \mathbb{Z}_3 + 3\mathcal{O}_{K,3}$  while  $R'' \cap K_3 = \mathcal{O}_{K,3}$ . Thus,  $R_0(36)_3$  is admissible for  $(\pi_{E,3}, \chi_{n,3})$ .  $\square$

Let  $\Omega^{(n)}$  denote the minimal real period of  $E^{(n)}$  and  $\Omega$  the one of  $E$ . Then  $\Omega^{(n)}\Omega^{(n^{-1})} = \Omega^2/N$  with  $N = p_1 \cdots p_k$ . Let  $\phi \in S_2(\Gamma_0(36))$  be the new form associated to the elliptic curve  $E/\mathbb{Q}$ .

**Corollary 3.8.** *The Heegner point  $z_n$  satisfies the following height formula*

$$\frac{L'(1, E^{(n)})L(1, E^{(n^{-1})})}{\Omega^{(n)}\Omega^{(n^{-1})}} = \frac{1}{27}\hat{h}_{\mathbb{Q}}(z_n).$$

*Proof.* The explicit formula in Theorem 3.5 implies the following identity

$$L'(1, E, \chi_n) = \frac{(8\pi^2)(\phi, \phi)_{U_0(36)}}{\sqrt{3} \cdot 3N} \cdot \frac{\langle P_{\chi_n}(f), P_{\chi_n^{-1}}(f) \rangle_{K,K}}{(f, f)_{\mathcal{R}^\times}},$$

where

$$P_{\chi_n}(f) = \sum_{t \in \widehat{K}^\times/K^\times \widehat{\mathcal{O}}_{3N}^\times} f(P_0)^{\sigma_t} \chi_n(t).$$

The order  $\mathcal{R}$  chosen in the introduction is conjugate to  $R_0(36)$  outside the place 2. Thus

$$(f, f)_{\mathcal{R}^\times} = \frac{\text{Vol}(X_{\mathcal{R}^\times})}{\text{Vol}(X_0(36))} \deg f = \frac{\text{Vol}(U_0(36)_2)}{\text{Vol}(\mathcal{R}_2^\times)} = \frac{1}{3}.$$

Let  $L = K(\sqrt[3]{n})$  and  $z = \text{Tr}_{H_{6N}/L} f(P_0)$ . When  $3 \nmid \sum_1^k \epsilon_i$ ,  $\text{Gal}(L/K) = \langle \sigma_{\omega_3} \rangle$ . Then

$$\begin{aligned} \langle P_{\chi_n}(f), P_{\chi_n^{-1}}(f) \rangle_{K,K} &= \frac{1}{9} \left\langle \sum_{\sigma \in \text{Gal}(L/K)} z^\sigma \chi_n(\sigma), \sum_{\sigma \in \text{Gal}(L/K)} z^\sigma \chi_n^{-1}(\sigma) \right\rangle_{K,K} \\ &= \frac{1}{3} (\langle z, z \rangle_{K,K} - \langle z^{\sigma_{\omega_3}}, z \rangle_{K,K}), \end{aligned}$$

By Corollary 2.6,  $z^{\sigma_{\omega_3}} \equiv [\omega]z \pmod{\text{torsions}}$ ,

$$\langle z^{\sigma_{\omega_3}}, z \rangle_{K,K} = \frac{1}{2} \left( \hat{h}_K([1+\omega]z) - \hat{h}_K([\omega]z) - \hat{h}_K(z) \right) = -\frac{1}{2} \langle z, z \rangle_{K,K}$$

and therefore

$$\langle P_{\chi_n}(f), P_{\chi_n^{-1}}(f) \rangle_{K,K} = \frac{1}{2} \hat{h}_K(z) = \hat{h}_{\mathbb{Q}}(z).$$

While we note that  $z_n = 3z$ ,

$$L'(1, E, \chi_n) = \frac{8\sqrt{3}\pi^2(\phi, \phi)_{U_0(36)}}{27N} \hat{h}_{\mathbb{Q}}(z_n).$$

Since

$$\Omega^{(n)}\Omega^{(n^{-1})} = \Omega^2/N = \frac{8\sqrt{3}\pi^2(\phi, \phi)_{U_0(36)}}{N},$$

we have

$$\frac{L'(1, E^{(n)})L(1, E^{(n^{-1})})}{\Omega^{(n)}\Omega^{(n^{-1})}} = \frac{1}{27}\hat{h}_{\mathbb{Q}}(z_n).$$

$\square$

Now assume  $k = 1$ . Let  $p \equiv 2, 5 \pmod{9}$  be a prime number and  $n = p^*$ . The point  $y_0 = \text{Tr}_{H_{3p}/K(\sqrt[3]{n})}(P_0 - T) \in E(K(\sqrt[3]{n}))$  is of infinite order and satisfies  $y_0^{\sigma_{\omega_3}} = [\omega]y_0 + t$ , with  $t \in E(\mathbb{Q})[\sqrt{-3}]$  non-zero. Then  $z_1 = \sqrt{-3}y_0$  is a point of infinite order in  $E(K(\sqrt[3]{n}))^{X^n}$ .

**Lemma 3.9.** *The point  $z_1$  is not divisible by  $\sqrt{-3}$  in  $E(K(\sqrt[3]{n}))^{X^n}$ .*

*Proof.* Assume  $z_1 = \sqrt{-3}Q + T$  with  $Q \in E(K(\sqrt[3]{n}))^\times$  and  $T \in E(K(\sqrt[3]{n}))_{\text{tor}}^{\chi_n}$ . Suppose that  $C$  is a large integer prime to 3. Then

$$\sqrt{-3}C(y_0 - Q) = CT$$

lies in  $E(K(\sqrt[3]{n}))[3]$ . Since  $E(K(\sqrt[3]{n}))[3^\infty] = E(K)[3]$ ,  $C(y_0 - Q)$  lies in  $E(K)[3]$  and assume  $Cy_0 = CQ + R$  with  $R \in E(K)[3]$ . Taking the Galois action of  $\sigma_{\omega_3}$ , we obtain

$$Ct = [1 - \omega]R = 0,$$

which is a contradiction.  $\square$

*Proof of Theorem 1.2.* We showed that  $\hat{h}_{\mathbb{Q}}(z_n) \neq 0$ . Therefore  $L'(1, E, \chi_n) = L'(1, E^{(n)})L(1, E^{(n^{-1})}) \neq 0$  and in particular we have  $\text{ord}_{s=1} L(s, E^{(n)}) = 1$  and  $\text{ord}_{s=1} L(s, E^{(n^{-1})}) = 0$ . By results of Gross-Zagier and Kolyvagin, we know  $\text{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 1$  and  $\text{III}(E^{(n)}/\mathbb{Q})$  is finite and that  $\text{rank}_{\mathbb{Z}} E^{(n^{-1})}(\mathbb{Q}) = 0$  and  $\text{III}(E^{(n^{-1})}/\mathbb{Q})$  is finite. Note that Tamagawa numbers  $c_v(E^{(n)}) = c_v(E^{(n^{-1})}) = 3$  for  $v \mid 2p$  and  $c_v(E^{(n)}) = c_v(E^{(n^{-1})}) = 1$  for other places  $v$ , and that  $E^{(n)}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$  and  $E^{(n^{-1})}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ . Then the BSD conjecture predicts

$$\text{BSD}(n) \quad L'(1, E^{(n)})/\Omega^{(n)} = \#\text{III}(E^{(n)})\hat{h}_{\mathbb{Q}}(P),$$

where  $P$  is the generator of the free part of  $E^{(n)}(\mathbb{Q})$ , and

$$\text{BSD}(n^{-1}) \quad L(1, E^{(n^{-1})})/\Omega^{(n^{-1})} = \#\text{III}(E^{(n^{-1})}).$$

Then  $\text{BSD}(n) \cdot \text{BSD}(n^{-1})$  is

$$L'(1, E, \chi_n)/\Omega^{(n)}\Omega^{(n^{-1})} = \#\text{III}(E^{(n^{-1})}) \cdot \#\text{III}(E^{(n)}) \cdot \hat{h}_{\mathbb{Q}}(P).$$

The descent method tells that

$$\dim_{\mathbb{F}_3} \text{Sel}_3(E^{(n)})/E^{(n)}(\mathbb{Q})_{\text{tor}} \leq 1 \text{ and } \dim_{\mathbb{F}_3} \text{Sel}_3(E^{(n^{-1})})/E^{(n^{-1})}(\mathbb{Q})_{\text{tor}} = 0.$$

Hence  $\text{III}(E^{(n)})[3^\infty] = \text{III}(E^{(n^{-1})})[3^\infty] = 0$ . Note  $z_n = 9y_0$ . By the explicit Gross-Zagier formula in Corollary 3.8 and the triviality of  $\text{III}(E^{(n)})[3^\infty]$  and  $\text{III}(E^{(n^{-1})})[3^\infty]$ , in order to prove the 3-part of  $\text{BSD}(n) \cdot \text{BSD}(n^{-1})$ , it suffices to show that  $\hat{h}_{\mathbb{Q}}(P) = u\hat{h}_{\mathbb{Q}}(z_1)$  with  $u \in \mathbb{Z}_3^\times \cap \mathbb{Q}$ .

Since the free part of  $E^{(n)}(K)$  has  $\mathcal{O}_K$ -rank 1, the ratio  $\hat{h}_{\mathbb{Q}}(P)/\hat{h}_{\mathbb{Q}}(z_1)$  is a rational number. Recall there is an isomorphism  $\phi : E^{(n)}(K) \simeq E(K(\sqrt[3]{n}))^{\chi_n}$  such that  $\phi(\overline{R}) = \overline{\phi(R)}$  for any point  $R \in E^{(n)}(\overline{\mathbb{Q}})$ . By Proposition 2.8,  $\overline{z_1} = z_1$  and hence  $\phi^{-1}(z_1)$  is rational over  $\mathbb{Q}$ . Since  $z_1$  is not divisible by  $\sqrt{-3}$  in  $E(K(\sqrt[3]{n}))^{\chi_n}$ ,  $\phi^{-1}(z_1) \equiv tP \pmod{\text{torsions}}$  with some  $t \in \mathbb{Z}_3^\times$ . Then  $\hat{h}_{\mathbb{Q}}(P) = u\hat{h}_{\mathbb{Q}}(z_1)$  with some  $u \in \mathbb{Z}_3^\times$ .  $\square$

## REFERENCES

- [1] Birch, B.J., *Elliptic curves and modular functions*, Symposia Mathematica, Indam Rome 1968/1969, vol. 4, pp27-32. London: Academic Press (1970).
- [2] Birch, B.J. and Swinnerton-Dyer, H.P., *Notes on elliptic curves (II)*, J. Reine Angew. Math, 218 (1965), 79-108.
- [3] L. Cai, J. Shu and Y. Tian *Explicit Gross-Zagier formula and Waldspurger formula*, 2014.
- [4] W. Casselman, *The restriction of a representation of  $\text{GL}_2(k)$  to  $\text{GL}_2(\mathcal{O})$* , Math. Ann. 206 (1973), 311-318.
- [5] John Coates, Yongxiong Li, Ye Tian, and Shuai Zhai, *Quadratic Twists of Elliptic Curves*, preprint.
- [6] S. Dasgupta and J. Voight *Heegner points and Sylvester's conjecture*, Arithmetic geometry, 91-102, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009.
- [7] B. Gross, *Heights and the special values of L-series*. Canadian Mathematical Society, Conference Proceedings, Volume 7 (1987).
- [8] B. Gross, *Local orders, root numbers, and modular curves*, American Journal of Mathematics, 110(1988), 1153-1182.
- [9] S. Gelbart and H. Jacquet, *A relation between automorphic representations of  $\text{GL}(2)$  and  $\text{GL}(3)$* , Ann. Sci. École Norm. Sup. (4) 11 (1978), no. 4, 471C542.
- [10] B. Gross and D. Prasad, *Test vectors for linear forms*, Math. Ann, 291(1991), 343-355.
- [11] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. 84 (1986), no. 2, 225-320.
- [12] Heegner, K. *Diophantische analysis und modulfunktionen*. Math. Z. 56, 227-253 (1952).
- [13] Shinichi Kobayashi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Preprint.
- [14] V.A.Kolyvagin, *Euler system*, The Grothendieck Festschrift. Prog. in math., Boston, Birkhauser (1990).
- [15] V.A.Kolyvagin, *Finiteness of  $E(\mathbb{Q})$  and  $\text{III}(E, \mathbb{Q})$  for a subclass of Weil curves*, Math. USSR Izvestiya, Vol. 32 (1989), No. 3.
- [16] D. Lieman, *Nonvanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. 140 (1994), 817-808.
- [17] Toshitsune Miyake, *Modular Forms*, Springer Monographs in Mathematics, 1989.
- [18] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Math. Z. 204, 45-68 (1990).
- [19] Jan Nekovář, *The Euler system method for CM points on Shimura curves*, In: L-functions and Galois representations, (Durham, July 2004), LMS Lecture Note Series 320, Cambridge Univ. Press, 2007, pp. 471 - 547.

- [20] Perrin-Riou, B., *Points de Heegner et dérivées de fonctions  $L$   $p$ -adiques*, Invent. Math. 89 (1987), no. 3, pp. 455-510.
- [21] Prasad, Dipendra, *Some applications of seesaw duality to branching laws*, Math. Ann. 304, 1-20 (1996).
- [22] H. Saito, *On Tunnell's formula for characters of  $GL(2)$* , Compositio Math. 85 (1993), 99-108.
- [23] P. Satge, *Un analogue du calcul de Heegner*, Inv. Math. 87 (1987), 425-439.
- [24] J. J. Sylvester, *On certain ternary cubic-form equations*, American Journal of Math. Vol 2, No 4. 1879, pp. 357-393.
- [25] J. Tate, *Number Theoretic Background in Automorphic Forms, Representations and  $L$ -functions*, Proc. Symp. in Pure Math. XXXIII Part 2(1979), 3-26.
- [26] Ye Tian, *Congruent Numbers with many prime factors*, PNAS, Vol 109, no. 52. 21256-21258.
- [27] Ye Tian, *Congruent Numbers and Heegner Points*, preprint.
- [28] Ye Tian, *Congruent Number Problem*, will appear in proceeding of ICCM 2013.
- [29] Ye Tian, Xinyi Yuan, and Shouwu Zhang, *Genus Periods, Genus Points, and Congruent Number Problem*, preprint.
- [30] J. Tunnell, *On the local Langlands conjecture for  $GL(2)$* , Inv. Math. 46 (1978), 179-200.
- [31] J. Tunnell, *Local  $\epsilon$ -factors and characters of  $GL(2)$* , Amer. J. Math. 105 (1983), 1277- 1307. [13]
- [32] Marie-France Vignéras, *Arithmétique des Algèbres de Quaternions*, Lecture Note of Mathematics, 800. Springer, Berlin, 1980. vii+169 pp.
- [33] X.Yuan, S. Zhang, and W. Zhang, *The Gross-Zagier formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2012.

LI CAI: MATHEMATICAL SCIENCES CENTER, TSINGHUA UNIVERSITY, BEIJING 100084  
*E-mail address:* `lcail@math.tsinghua.edu.cn`

JIE SHU: ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE, MORNINGSIDE CENTER OF MATHEMATICS, CHINESE ACADEMY OF SCIENCES, BEIJING 100190  
*E-mail address:* `shujie09@mails.gucas.ac.cn`

YE TIAN: ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE, MORNINGSIDE CENTER OF MATHEMATICS, CHINESE ACADEMY OF SCIENCES, BEIJING 100190  
*E-mail address:* `ytian@math.ac.cn`